CYBERSECURITY & PRIVACY

2021 Healthcare Compliance Webinar

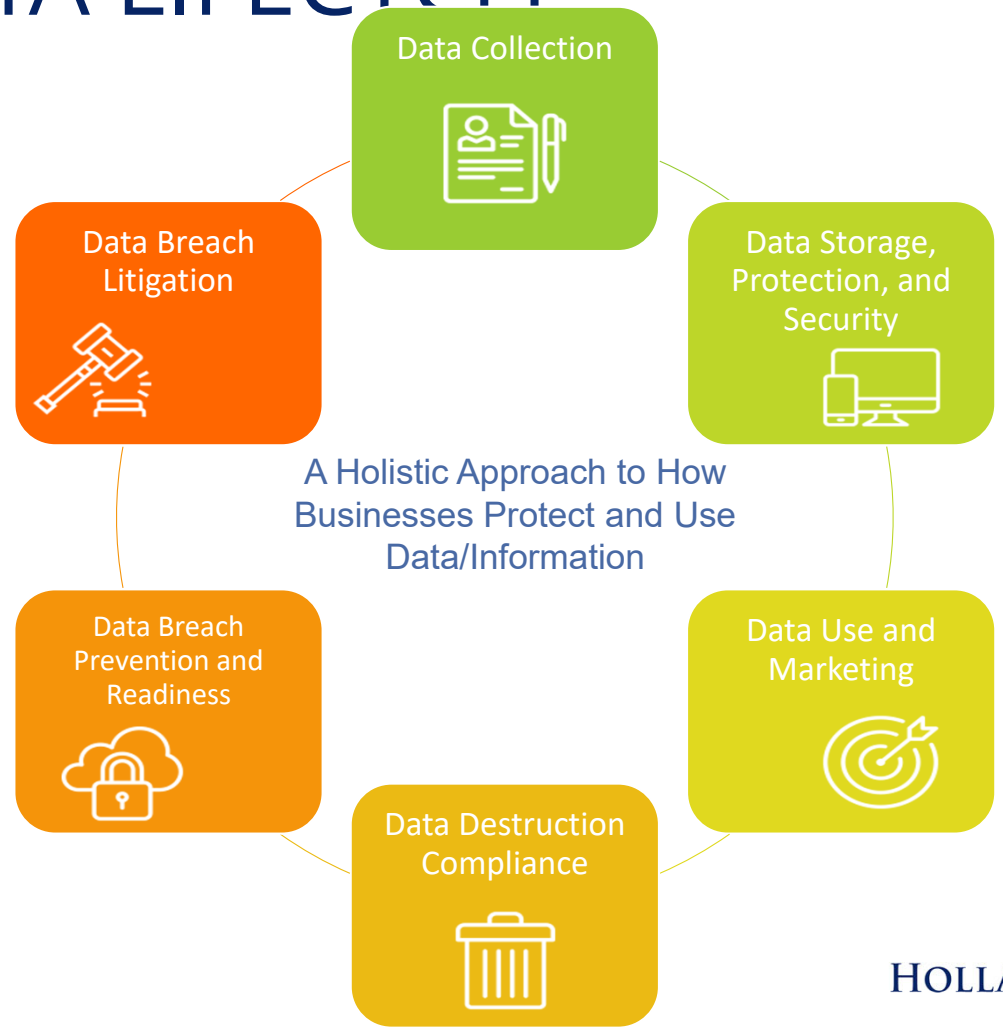
February 4, 2021

HOLLAND&HART LLP

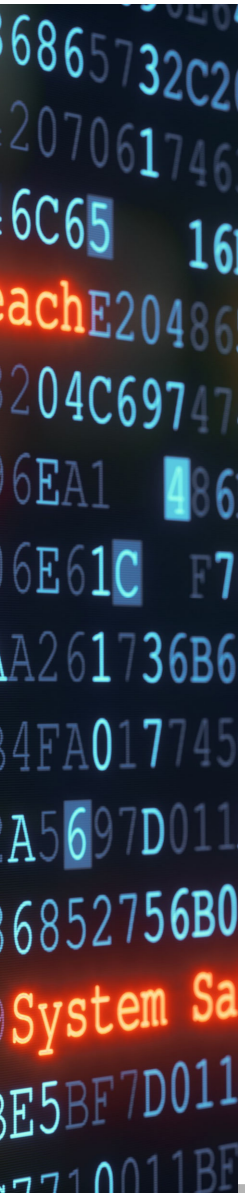
DISCLAIMER

This presentation is similar to any other seminar designed to provide general information on pertinent legal topics. The statements made and any materials distributed as part of this presentation are provided for educational purposes only. They do not constitute legal advice nor do they necessarily reflect the views of Holland & Hart LLP or any of its attorneys other than the speakers. This presentation is not intended to create an attorney-client relationship between you and Holland & Hart LLP. If you have specific questions as to the application of the law to your activities, you should seek the advice of your legal counsel.

THE DATA LIFECYCLE



HOLLAND&HART



THE AGENDA

- The Threats
- The Guidance
- The Breach

HOLLAND&HART LLP

2020 VERIZON DATA BREACH STUDY

C-Suite executives are 12 time more likely to be targeted in social engineering attacks than other employees

Cyber-espionage related data breaches increased from 13% of breaches in 2017 to 25% in 2018

Nation-state attacks increased from 12% of attacks in 2017 to 23% in 2018

Financial breaches to

Phishing is involved in 32% of breaches and 78% of cyber-espionage incidents

90% of malware arrived via email

60% of web application attacks were on cloud-based email servers

Most ema BEC at resulte breache mult authentica been im

45% of cyberattacks involve hacking

30% of attacks involved insiders

43% of cyberattacks were on small businesses

Ransom second big threat an for 24% related

There has been a six-fold decrease in attacks on HR personnel

Misconfiguration of cloud platforms accounted for 21% of breaches caused by errors

Source: 2020 Verizon Data Breach Investigations Report

VERIZON DATA BREACH STUDY

45% of all reported breaches featured hacking

Errors were the cause of 22% of reported breaches

70% were caused by external actors and bad guys

Organiz groups w 55% of

22% of breaches involved social attacks, such as phishing

30% involved internal actors

17% involved malware

27% of t incide ransomw of

Web applications were involved in 43% of breaches

37% of breaches stole or used stolen credentials

28% of breaches involved small business victims

58% of perso comp

There has been a six-fold decrease in attacks on HR personnel

Misconfiguration of cloud platforms accounted for 26% of breaches caused by errors (increase of 5 %)

Source: 2020 Verizon Data Breach Investigations Report

VERIZON DATA BREACH STUDY

- Substantial increase in the number of reported breac and incidents in the Healthcare industry, rising to 521 breaches and incidents as compared to 304 in the 20 report.
- Out of all industry sectors analyzed, healthcare was th only industry where the number of incidents caused b insiders was greater than those caused by external th actors. 51% of incidents involved internal actors as compared to 48% (in 2019, 59% of incidents involved insiders compared to 42% involving external threat actors).
- The primary motive for attacks on the healthcare indu was financial gain (88%), followed by fun (4%), convenience (3%). 67% of breaches involved medical data, 77% involved personal information, and 18% involved credential theft.
- Privilege misuse dropped significantly, down to 8.7 % incidents as compared to 23% in the 2019 report. Question: does that mean misuse of privilege inciden are dropping? Or does it mean that because ransomw incidents have increased significantly, they have simp dropped in proportion to the rise in ransomware?
- *Source: 2020 Verizon Data Breach Investigations Report*

GREY + SLOAN MEMORIAL HOSPITAL

REAL WORLD SCENARIO

HOLLAND & HART LLP

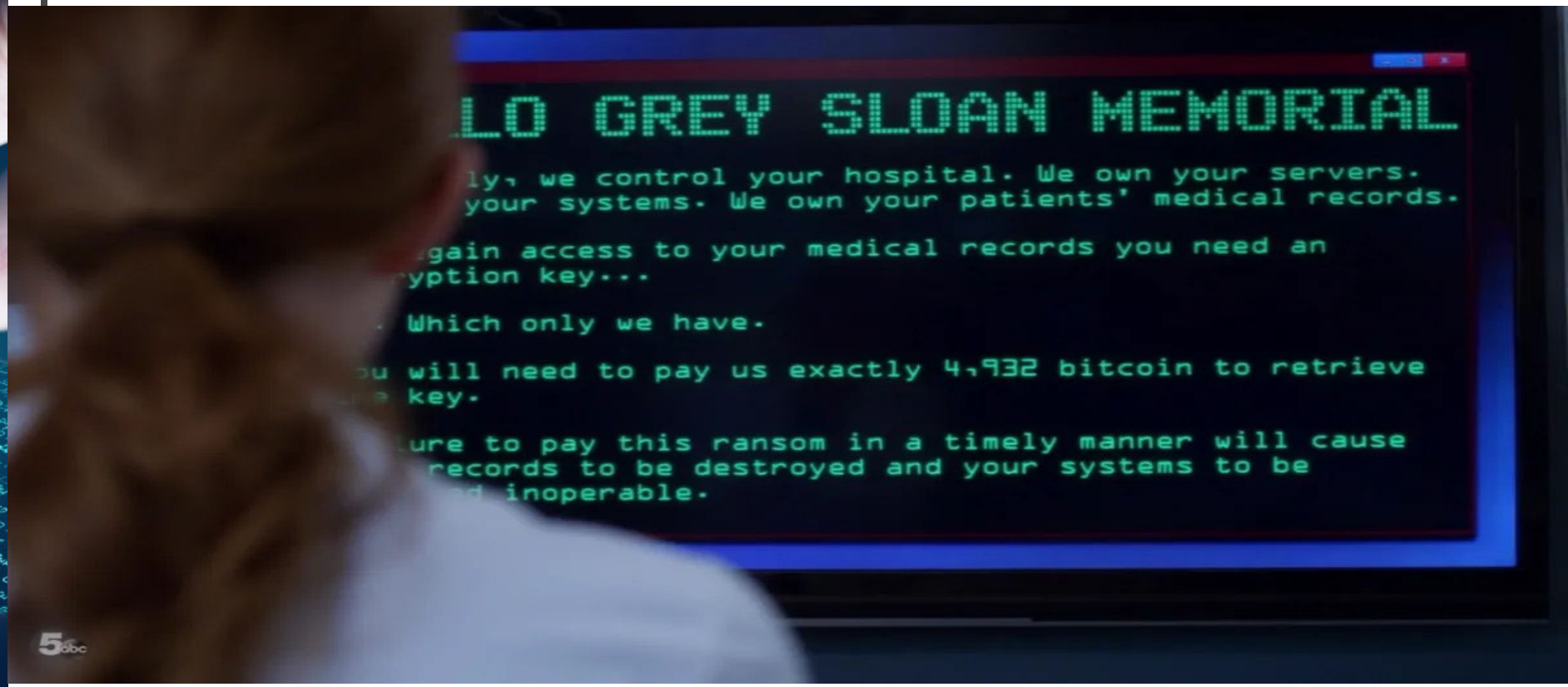
RANSOMWARE

- You're in the ER looking over an elderly patient on a cardiac monitor. The alarm sounds . . . He's flatlining. Dr. Owen Hunt calls for a crash cart, pulls out the paddles and . . .
- Suddenly, all of the patient's monitors go haywire. They are all flatlining. Is it possible?

RANSOMWARE

- In the OR, Dr. Meredith Grey is performing an operation in a woman with an enlarged spleen. The OR monitors start to flicker and malfunction . . . In the middle of surgery.
- Dr. Miranda Bailey sits down at a computer workstation in order to access the hospital's EHR system. She gets an error message . . . Access is denied.
- And then this . . .

RANSOMWARE



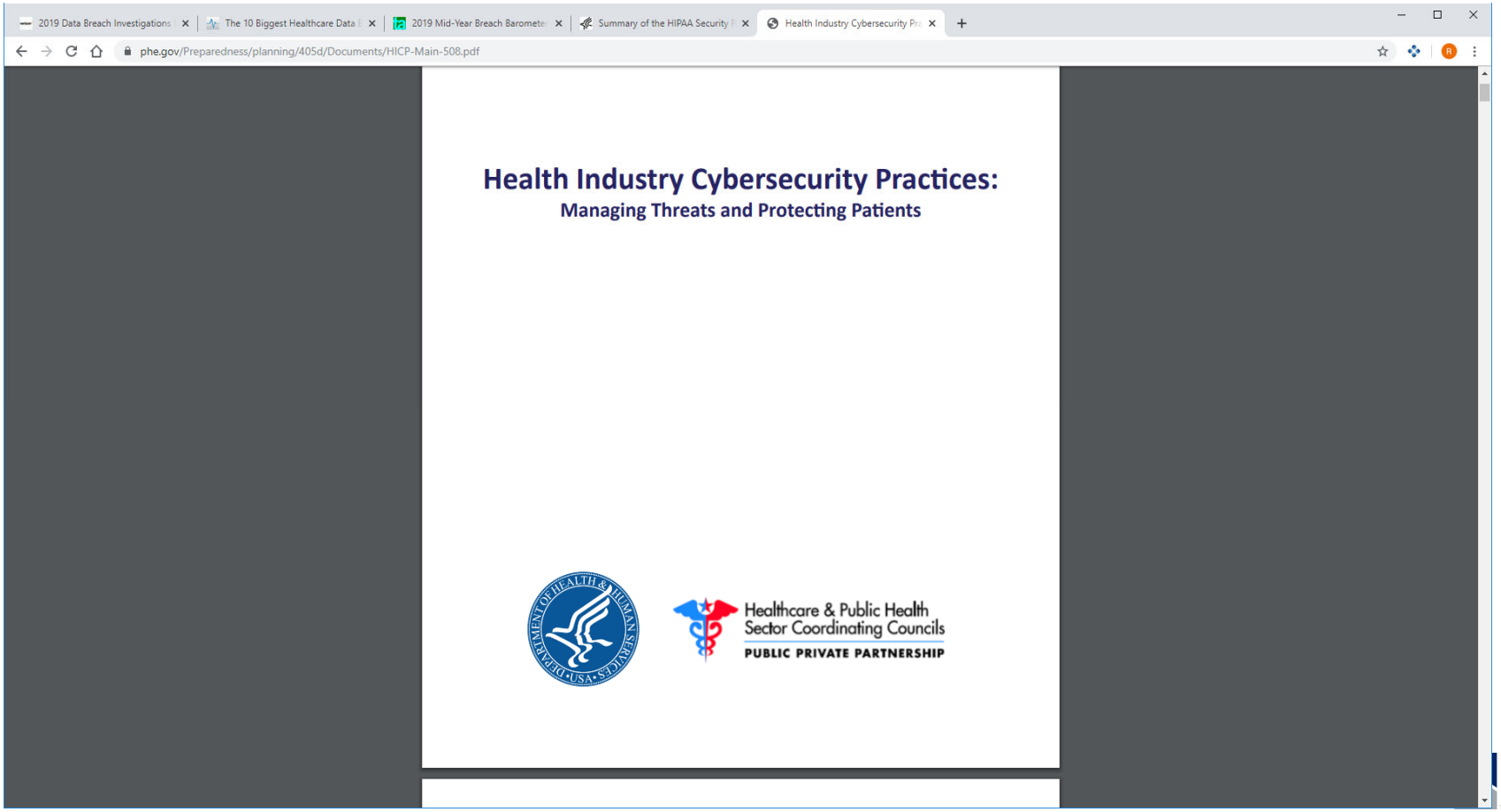
Source: Grey's Anatomy, "Out of Nowhere", Season 14, Episode 8, ABC Television

HOLLAND&HART LLP

THE GUIDANCE

HOLLAND&HART LLP

HHS GUIDANCE ON CYBERSECURITY PROTECTION



THE GUIDANCE

- *"To adequately maintain patient safety and protect our sector's information and data, there must be a culture change and an acceptance of the importance and necessity of cybersecurity as an integrated part of patient care. The changes and the resulting effort required will not abate, but will rather change with the times, technologies, threats, and events. Now is the time to start, and, together, we can achieve real results"*

5 CURRENT THREATS

- E-mail phishing attack
- Ransomware attack
- Loss or theft of equipment or data
- Insider, accidental or intentional data loss
- Attacks against connected medical devices that may affect patient safety

THREAT: E-MAIL PHISHING ATTACK

- Real-World Scenario: Your employees receive a fraudulent e-mail from a cyber-attacker disguised as an IT support person from your patient billing company. The e-mail instructs your employees to click on a link to change their billing software passwords. An employee who clicks the link is directed to a fake login page, which collects that employee's login credentials and transmits this information to the attackers. The attacker then uses the employee's login credentials to access your organization's financial and patient data. Impact: A pediatrician learns that an attacker stole patient data using a phishing attack and used it in an identity theft crime.
- Impact: A pediatrician learns that an attacker stole patient data using a phishing attack and used it in an identity theft crime.

HOLLAND&HART LLP

THREAT: E-MAIL PHISHING ATTA

- On average, a person will receive about 80 e-mails per day. Knowin

are safe to open can get tricky if you are not asking yourself the follow

questions:

  - Do you know the sender?
  - Are there any spelling or grammatical errors, or any other indica

    the tone or style of the e-mail is off?
  - Before clicking on a link, did you hover over it to see the URL des
  - Do you know the sender, or are you suspicious of the e-mail? If i

    do NOT open any attachments. •
  - What are my organization's processes for reporting suspicious e-

- The best time to familiarize yourself with your organization's policie

reporting a suspicious e-mail is when you begin employment. Whenev

receive an e-mail that sounds too good to be true or that you were no

expecting, verify it before opening it!

- Check with colleagues to find out whether they received the same

mail. You can always seek the guidance of your IT security support tea

similar point of contact. Talk to them to find out whether your accoun

protected with the proper security filters to ward off unwanted junk n

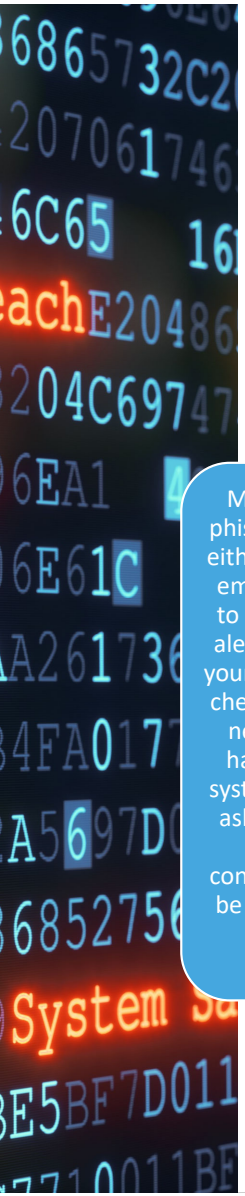
THREAT: E-MAIL PHISHING ATTACK

Be	Be suspicious of e-mails from unknown senders, e-mails that request sensitive information such as PHI or personal information, or e-mails that include a call to action that stresses urgency or importance (1.S.B)
Train	Train staff to recognize suspicious e-mails and to know where to forward them (1.S.B)
Open	Never open e-mail attachments from unknown senders (1.S.B)
Tag	Tag external e-mails to make them recognizable to staff (1.S.A)
Implement	Implement incident response plays to manage successful phishing attacks (8.M.A)
Implement	Implement advanced technologies for detecting and testing e-mail for malicious content or links (1.L.A)
Implement	Implement multifactor authentication (MFA) (1.S.A, 3.M.D)
Implement	Implement proven and tested response procedures when employees click on phishing e-mails (1.S.C)
Establish	Establish cyber threat information sharing with other health care organizations (8.S.B, 8.M.C)

THREAT: RANSOMWARE ATTACK

- Real-World Scenario: Through an e-mail that appears to have originated from a credit card company, a user is directed to a fake website and tricked into downloading a security update. The so-called security update is actually a malicious program designed to find and encrypt data, rendering them inaccessible. The program then instructs the user to pay a ransom to unlock or unencrypt the data.

- Impact: A practitioner cannot view patient charts because of a ransomware attack that has made the EHR system inaccessible.



REAT: RANSOMWARE ATTACK

Most ransomware attacks are sent in phishing campaign e-mails asking you to either open an attachment or click on an embedded link. Be sure you know how to identify these phishing e-mails! Stay alert when any e-mail asks you to enter your credentials. As a proactive measure, check to see whether the computer and network to which you are connected have the proper intrusion prevention system or software in place. That means asking • Do I have a high-performance firewall? • Do I have my firewall configured to only allow certain ports to be open? • Is there training I should be aware of to understand my organization's security policies?

Provide user awareness and compliance training during the onboarding process or when purchasing a new laptop or desktop equipment. If you discover that your computer has been infected, immediately disconnect from the network and notify your IT security team. Do not power off or shut down the computer or server, in case a volatile (RAM) memory image needs to be collected for forensics and incident response investigations

Due to the severity and time sensitivity of ransomware attacks, it is in your best interest and that of your organization to always seek out professional IT security or a similar point of contact help when you think your computer is infected with ransomware.

THREAT: RANSOMWARE ATTACK

- Ensure that users understand authorized patching procedures (7.S.A)
- Patch software according to authorized procedures (7.S.A)
- Be clear which computers may access and store sensitive or patient data (4.M.C)
- Use strong/unique username and passwords with MFA (1.S.A, 3.S.A, 3.M.C)
- Limit users who can log in from remote desktops (3.S.A, 3.M.B)
- Limit the rate of allowed authentication attempts to thwart brute-force attacks (3.M.C) Deploy anti-malware detection and remediation tools (2.S.A, 2.M.A, 3.L.D)
- Separate critical or vulnerable systems from threats (6.S.A, 6.M.B, 6.L.A)
- Maintain a complete and updated inventory of assets (5.S.A, 5.M.A)
- Implement a proven and tested data backup and restoration test (4.M.D)
- Implement a backup strategy and secure the backups, so they are not accessible on the network they are backing up (4.M.D)
- Implement proven and tested incident response procedures (8.S.A, 8.M.B)
- Establish cyber threat information sharing with other health care organizations (8.S.B, 8.M.C)
- Develop a ransomware recovery playbook and test it regularly (8.M.B)
- Once ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures (HHS Ransomware Fact Sheet)

THREAT: LOSS OR THEFT OF EQUIPMENT OR DATA

- Real-World Scenario: A physician stops at a coffee shop for a coffee and to use the public Wi-Fi to review radiology reports. As the physician leaves the table momentarily to pick up his coffee, a thief steals the laptop. The doctor returns to the table to find the laptop is gone.
- Impact: Loss of sensitive data may lead to a clear case of patient identity theft, and, with thousands of records potentially stolen, the physician's reputation could be at stake if all the patient records make it to the dark web for sale.

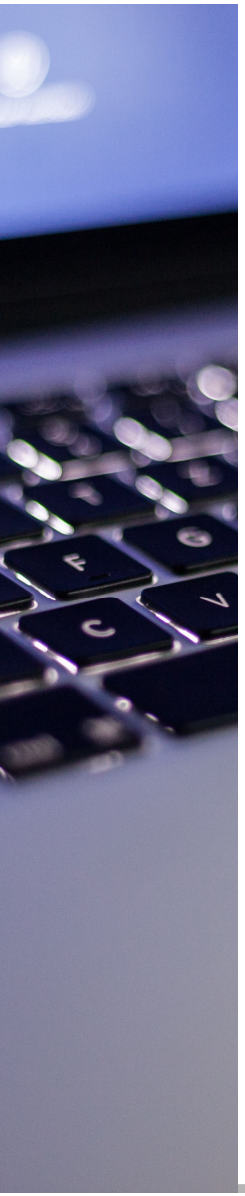
THREAT: LOSS OR THEFT OF EQUIPMENT OR DATA

Heading out on a business trip or a personal holiday? You need to follow the same, and maybe greater, security procedures as you do in the office. Make sure you know your organization's policy on removing equipment from the workplace by asking: • Can I travel with my equipment? • Can I take my equipment offsite to work remotely? • Are USB or other portable storage devices allowed? • Is the information on my computer or storage device encrypted? • Is there a secure virtual private network (VPN) that I can use, along with secure, passwordprotected Wi-Fi, to log into the network and work?

As soon as you realize that your device or equipment has been stolen or misplaced, your supervisor and IT security professional should be notified immediately so appropriate measures can be taken to safeguard the data saved on your device or equipment.

Your IT security support staff or similar point of contact should be notified when a work device or equipment has been misplaced, lost, or stolen. The data saved on them are now compromised and susceptible to unauthorized access, dissemination, and use. This is a serious cyber breach and should be handled by trained IT security professionals.

HOLLAND&HART LLP



THREAT: LOSS OR THEFT OF EQUIPMENT OR DATA

- Encrypt sensitive data, especially when transmitting data to other devices or organizations (4.S.B, 4.M.C)
- Implement proven and tested data backups, with proven and tested restoration of data (4.M.D)
- Acquire and use data loss prevention tools (4.M.E, 4.L.A)
- Implement a safeguards policy for mobile devices supplemented with ongoing user awareness training on securing these devices (9.M.A)
- Promptly report loss/theft to designated company individuals to terminate access to the device and/or network (3.S.A)
- Maintain a complete, accurate, and current asset inventory to mitigate threats, especially the loss and theft of mobile devices such as laptops and USB/thumb drives (5.S.A)
- Encrypt data at rest on mobile devices to be inaccessible to anyone who finds the device (4.M.C)
- Define a process with clear accountabilities to clean sensitive data from every device before it is retired, refurbished, or resold (5.S.C, 5.M.D)

HOLLAND&HART LLP

THREAT: INSIDER, ACCIDENTAL, OR INTENTIONAL DATA LOSS

- Real-World Scenario: An attacker impersonating a staff member of a physical therapy center contacts a hospital employee and asks to verify patient data. Pretending to be hospital staff, the imposter acquires the entire patient health record.
- Impact: The patient's PHI was compromised and used in an identity theft case.

THREAT: INSIDER, ACCIDENTAL OR INTENTIONAL DATA LOSS

See something? Say something! Follow your instinct, and always report what does not look or feel right to you. Beware of social engineering techniques. Check to see whether your organization conducts enhanced employee and vendor screening to make sure that those gaining access to company data are who they say they are and that they truly require access to the information. Are you limiting access to information to those who require it based on roles and responsibilities?

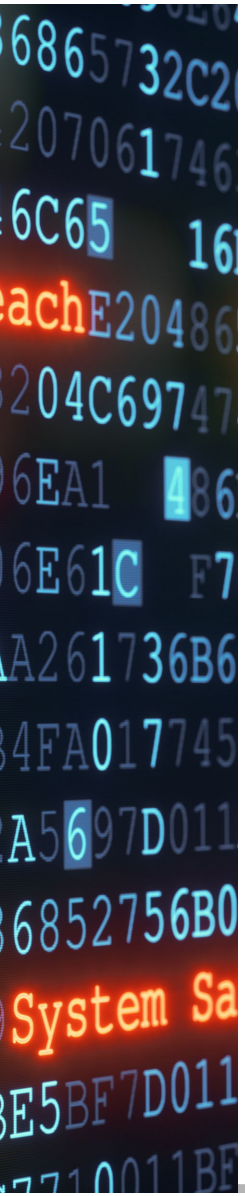
Conduct regular security training sessions to further employees' education and awareness. Train and test your staff to make sure they understand the security risks and the consequences of falling victim to insider attack. By doing so, you can lower the probability of such attacks happening in your organization.

Always consult your IT security professionals when exposed to a situation of stolen data or employee misconduct. Every situation will vary so your IT security professionals will be able to guide you best because a cyber-threat is not limited to hacking.

HOLLAND&HART LLP

THREAT: INSIDER, ACCIDENTAL OR INTENTIONAL DATA LOSS

Train	Train staff and IT users on data access and financial control procedures to mitigate social engineering or procedural errors (1.S.B, 1.M.D)
Implement and use	Implement and use workforce access auditing of health record systems and sensitive data (3.M.B)
Implement and use	Implement and use privileged access management tools to report access to critical technology infrastructure and systems (3.M.C)
Implement and use	Implement and use data loss prevention tools to detect and block leakage of PHI and PII via e-mail and web uploads (4.M.E, 4.L.A)

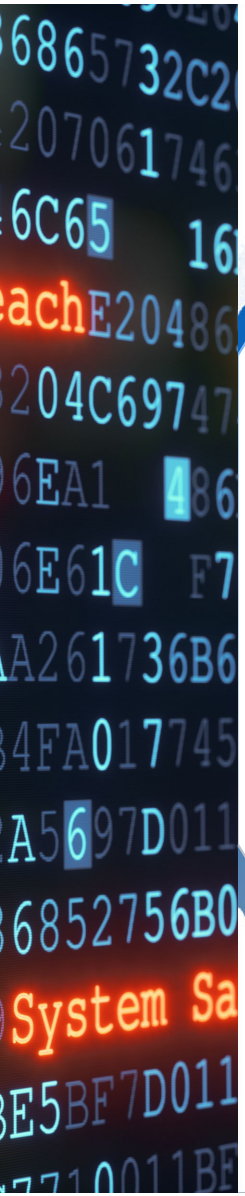


THREAT: ATTACKS AGAINST CONNECTED MEDICAL DEVICES THAT MAY AFFECT PATIENT SAFETY

Real-World Scenario: A cyber attacker gains access to a care provider's computer network through an e-mail phishing attack and takes command of a file server to which a heart monitor is attached. While scanning the network for devices, the attacker takes control (e.g., power off, continuously reboot) of all heart monitors in the ICU, putting multiple patients at risk.

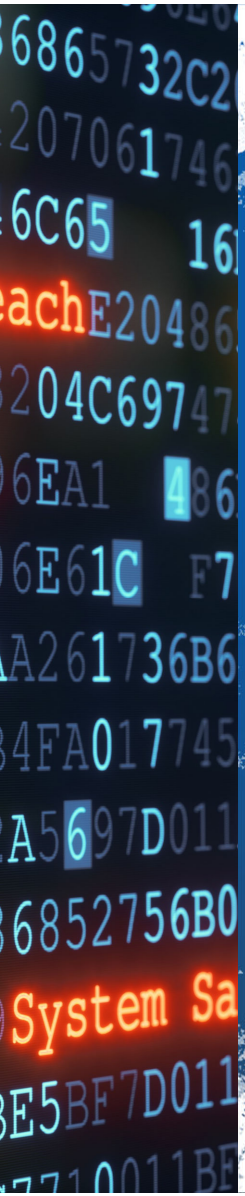
Impact: Patients are at great risk because an attack has shut down heart monitors, potentially during surgery and other procedures.

HOLLAND&HART LLP



THREAT: ATTACKS AGAINST CONNECTED MEDICAL DEVICES THAT MAY AFFECT PATIENT SAFETY

- Know your organization's protocols in case of a potential shutdown or attack against medical devices. Help patients and staff by understanding the processes and procedures; this can help mitigate the impacts. That means asking • How d we notify patients if their medical devices are compromised? • How do patient notify us if they suspect their medical devices are compromised?
- Knowledge of your organization's protocols for potential attacks on medical devices should be shared during new hire orientation or at security training. These protocols need to be communicated to patients when they are given medical devices.
- Each organization should have IT security professionals to help answer any questions on the policy and governance associated with medical devices. If you organization does not, ask your supervisor for information and/or resources allowing you to learn more about the threat. Vendors or manufacturers of medical devices may need to be engaged to understand vulnerabilities, risks, ar appropriate protection and response measures.



THREAT: ATTACKS AGAINST CONNECTED MEDICAL DEVICES THAT MAY AFFECT PATIENT SAFETY

- Establish and maintain communication with medical device manufacturer's product se teams (9.L.A)
- Patch devices after patches have been validated, distributed by the medical device manufacturer, and properly tested (9.M.B)
- Assess current security controls on networked medical devices (9.M.B, 9.M.E)
- Assess inventory traits such as IT components that may include the Media Access Con (MAC) address, Internet Protocol (IP) address, network segments, operating systems, applications, and other elements relevant to managing information security risks (9.M
- Implement pre-procurement security requirements for vendors (9.L.C)
- Implement information security assurance practices, such as security risk assessments
- new devices and validation of vendor practices on networks or facilities (1.L.A)
- Engage information security as a stakeholder in clinical procurements (9.L.C)
- Use a template for contract language with medical device manufacturers and others (9
- Implement access controls for clinical and vendor support staff, including remote acce monitoring of vendor access, MFA, and minimum necessary or least privilege (9.M.C)
- Implement security operations practices for devices, including hardening, patching, monitoring, and threat detection capabilities (9.L.B)
- Develop and implement network security applications and practices for device networ (9.M.E)

HIPAA SECURITY RULE

General requirements:	(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains or transmits
	(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information
	(3) Protect against any reasonably anticipated unauthorized uses or disclosures of such information
	(4) Workforce compliance

HIPAA SECURITY RULE

Requires compliance with security standards and required and addressable implementation specifications

Flexible approach:

- (1) May choose security measures that are reasonable and appropriate
- (2) Factors to consider:
  - size, complexity and capabilities
  - technical infrastructure, hardware and software security capabilities
  - costs of security measures
  - probability and criticality of potential risks to ePHI

HIPAA SECURITY RULE

Requires regular review and modification of security measures

Requires documenting actions, activities, assessments, policies and procedures in writing

- Retain for 6 years
- Make available to people implementing procedures
- Review periodically and update as needed

ADMINISTRATIVE SAFEGUARDS

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement.	164.308(b)(1)	Written Contract or Other Arrangement (R)

Source: https://www.gpo.gov/fdsys/pkg/CFR-2010-title45-vol1/pdf/CFR-2010-title45-vol1-part164-subpartC-appA.pdf

PHYSICAL SAFEGUARDS

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)

Source: https://www.gpo.gov/fdsys/pkg/CFR-2010-title45-vol1/pdf/CFR-2010-title45-vol1-part164-subpartC-appA.pdf

TECHNICAL SAFEGUARDS

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Technical Safeguards (see § 164.312)		
Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)

Source: https://www.gpo.gov/fdsys/pkg/CFR-2010-title45-vol1/pdf/CFR-2010-title45-vol1-part164-subpartC-appA.pdf

HHS RISK ASSESSMENT TOOL

Security Risk Assessment Tool

healthit.gov/providers-professionals/security-risk-assessment-tool

- Windows and iPad version
- Paper versions
- User guide
- No guarantee of compliant results
- Can document answers, comments and plans in tool

NIST 800-30 RISK ASSESSMENT PROCESS

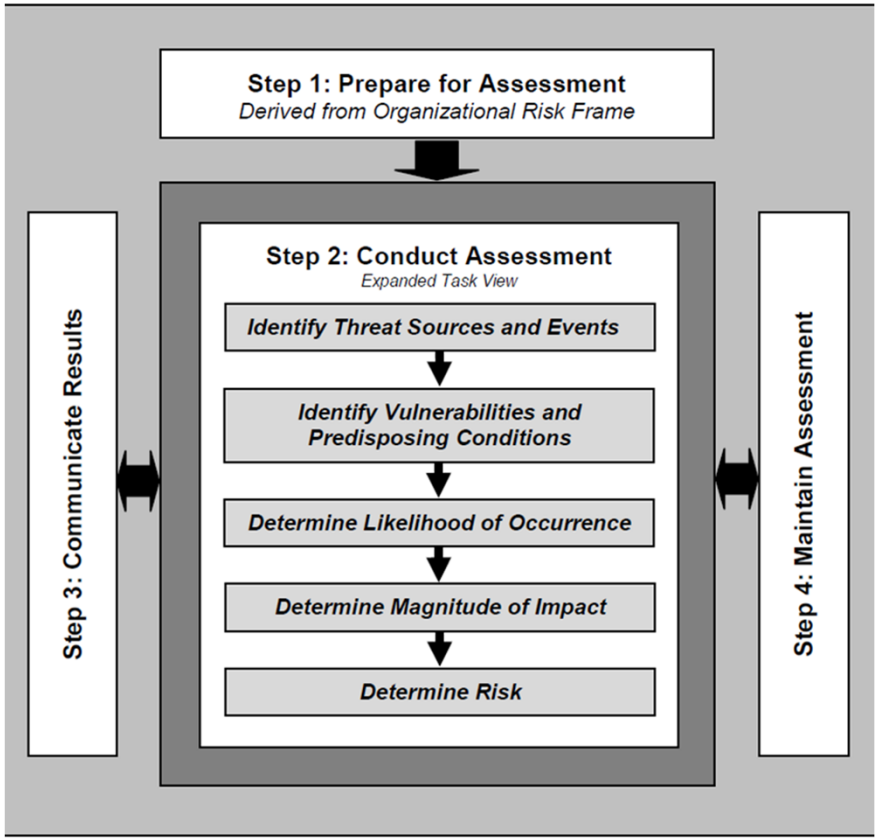
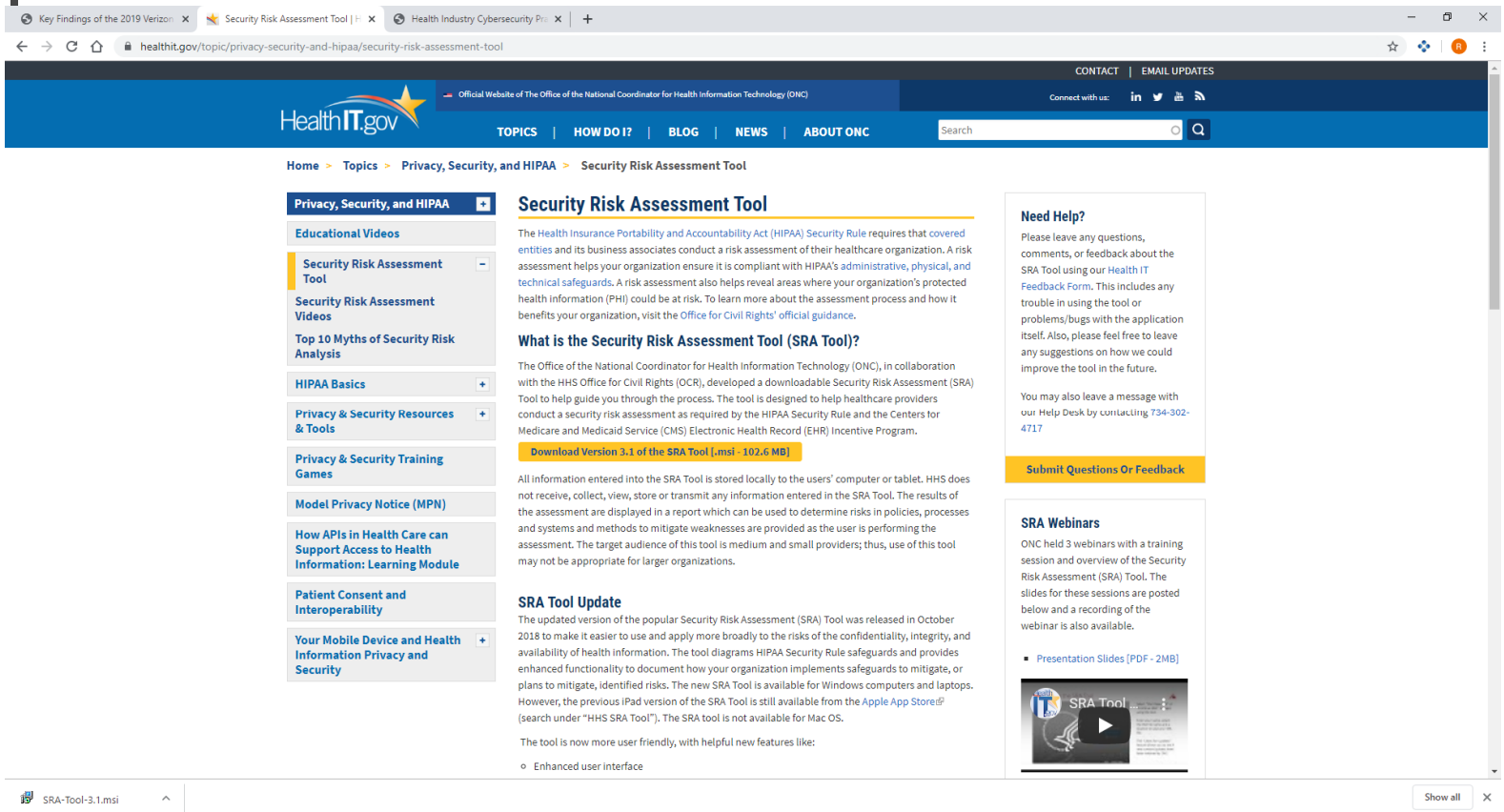
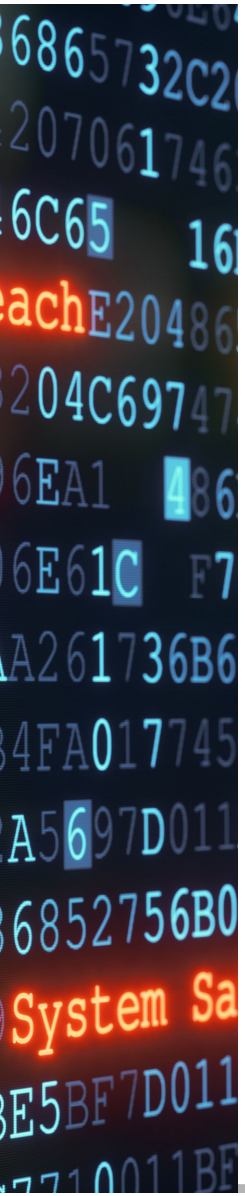


FIGURE 5: RISK ASSESSMENT PROCESS

HHS RISK ASSESSMENT TOOL



HOLLAND&HART LLP



INTERNAL DILIGENCE

What data do you have and where is it located?

Where does data originate and get stored, when do you delete, to whom do you transfer?

What are your access control "touch points?"

- Who can access data?
- How can they access it?
- What are the business needs for accessing it?

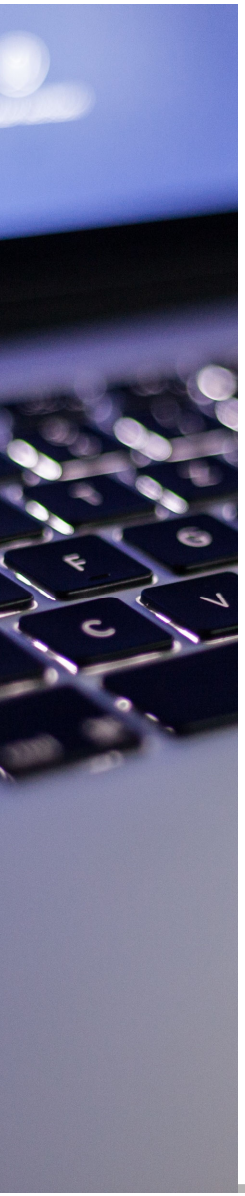
What are your policies, procedures and rules?

What do you need to be compliant with, and are you?

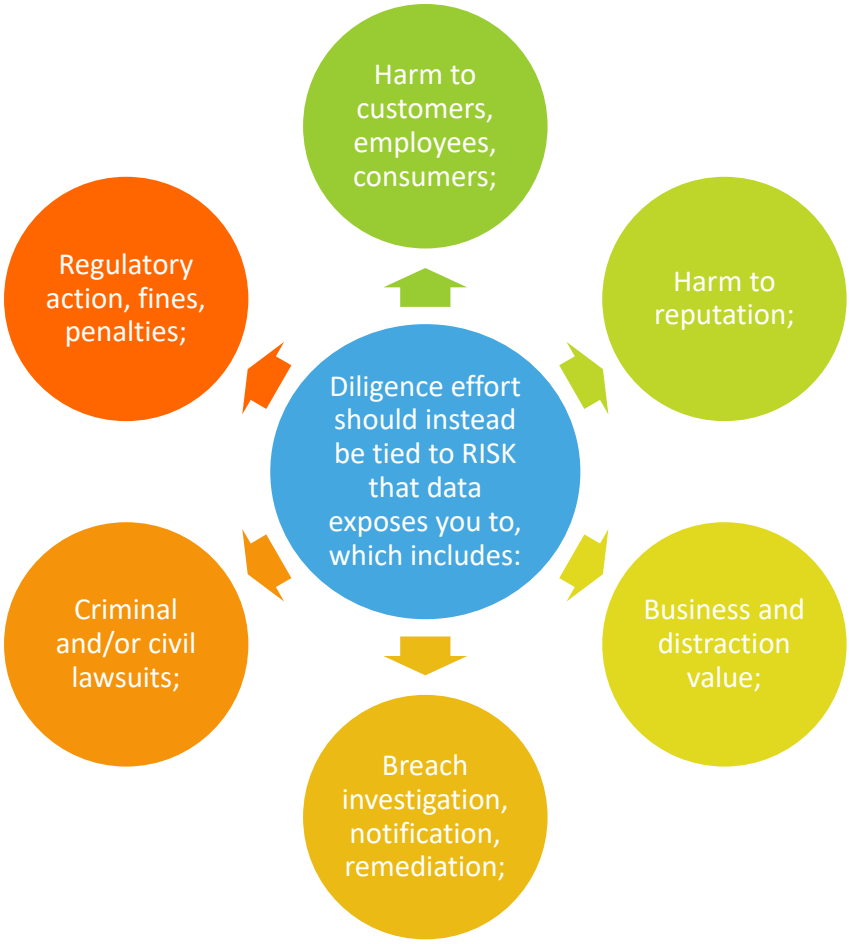
What security methodology and standards do you follow?

INTERNAL DILIGENCE

HOLLAND&HART LLP



EFFORT LEVEL = RISK LEVEL

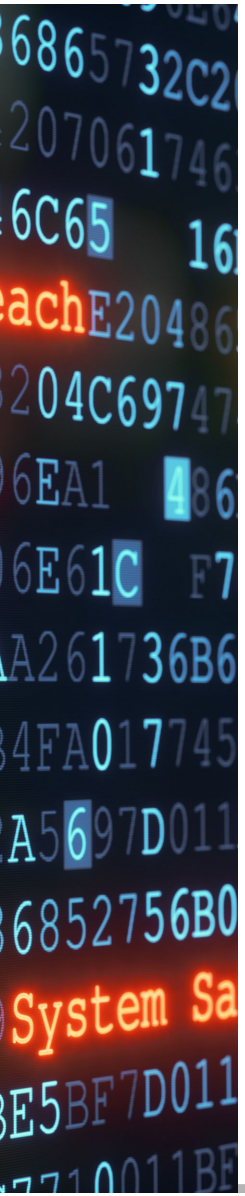


HOLLAND&HART LLP

CONTRACT NEGOTIATIONS:

Important Considerations:

- Risk allocation and liability;
- Audit and verification rights;
- Business Continuity/Disaster Recovery;
- Subcontractors, off-shoring;
- Data breach response and remediation;
- Information deletion or return;
- Compliance with laws, standards, policies, controls;
- Bankruptcy;
- Insurance;
- Termination/Unwind;



DO YOUR SOCs MATCH YOUR OUTFIT?

What security methodology and standards do they follow?

SOC 1, 2, 3	ISO/IEC 27000/27001	PCI	NIST Cybersecurity Framework

How do they verify/audit compliance?

How frequently do they audit?

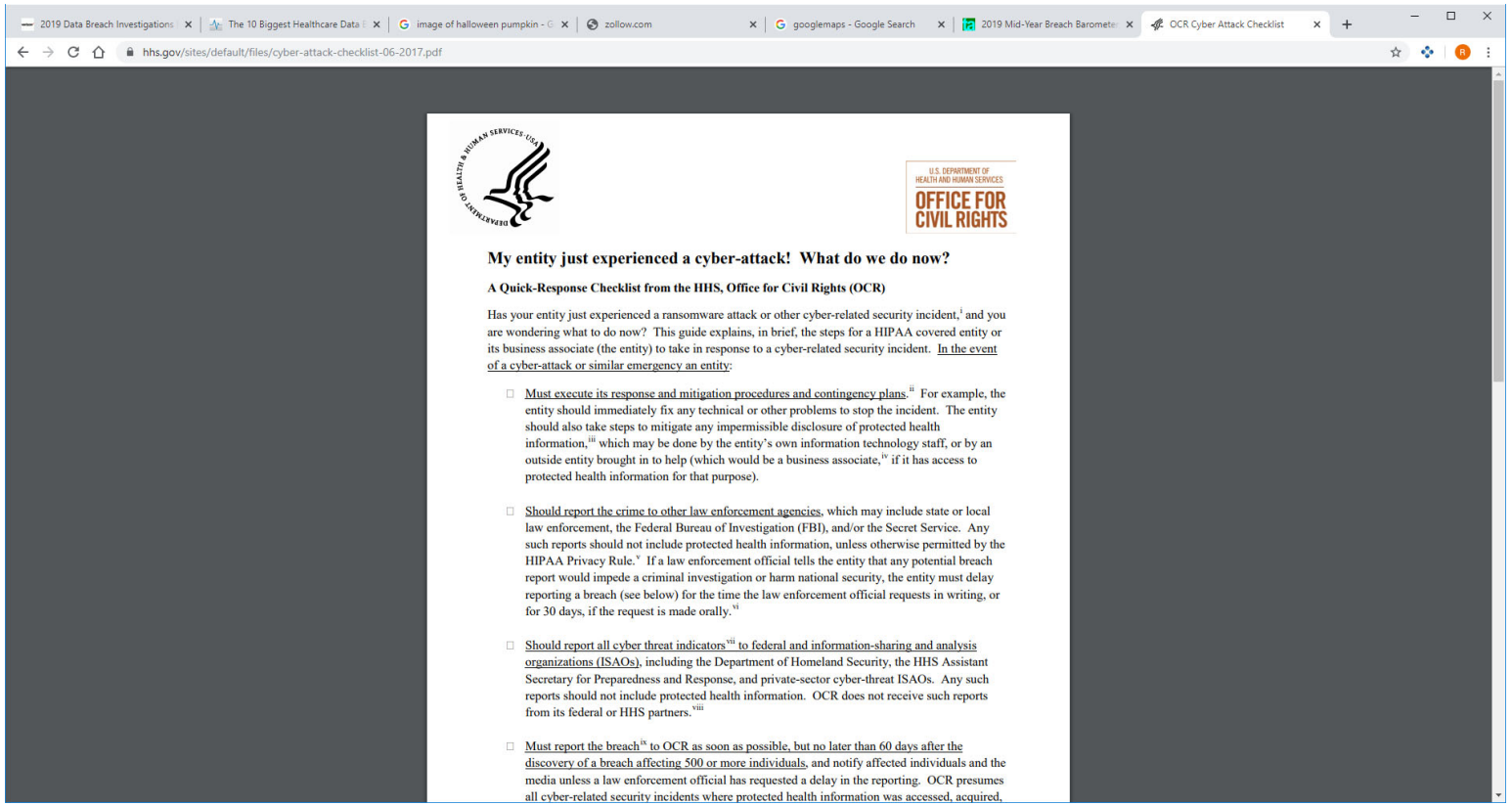
Do they have certification?

What is the scope of the audit?

DATA BREACHES, HOW THEY HURT

- Business Disruption
- Reputational Harm
- Multi-faceted Litigation

THE GUIDANCE



2019 Data Breach Investigations | The 10 Biggest Healthcare Data | image of halloween pumpkin - G | zollow.com | googlemaps - Google Search | 2019 Mid-Year Breach Barometer | OCR Cyber Attack Checklist

hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

My entity just experienced a cyber-attack! What do we do now?

A Quick-Response Checklist from the HHS, Office for Civil Rights (OCR)

Has your entity just experienced a ransomware attack or other cyber-related security incident,[i] and you are wondering what to do now? This guide explains, in brief, the steps for a HIPAA covered entity or its business associate (the entity) to take in response to a cyber-related security incident. In the event of a cyber-attack or similar emergency an entity:

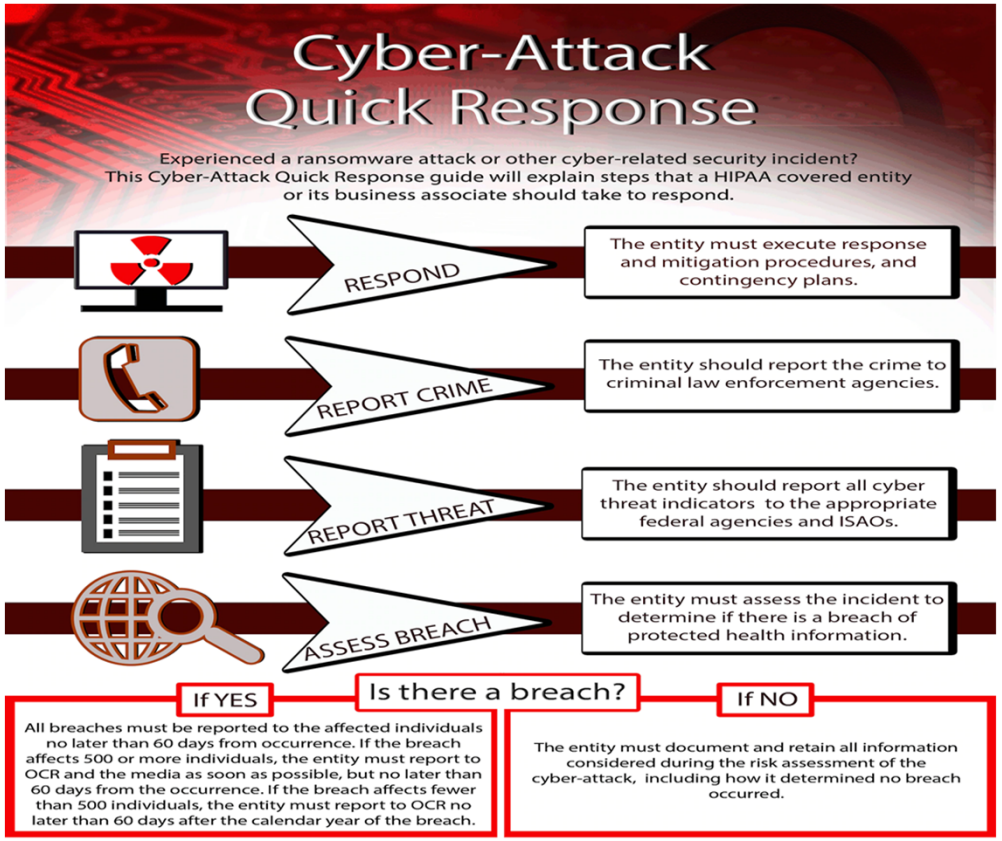
- ☐ Must execute its response and mitigation procedures and contingency plans.[ii] For example, the entity should immediately fix any technical or other problems to stop the incident. The entity should also take steps to mitigate any impermissible disclosure of protected health information,[iii] which may be done by the entity's own information technology staff, or by an outside entity brought in to help (which would be a business associate,[iv] if it has access to protected health information for that purpose).

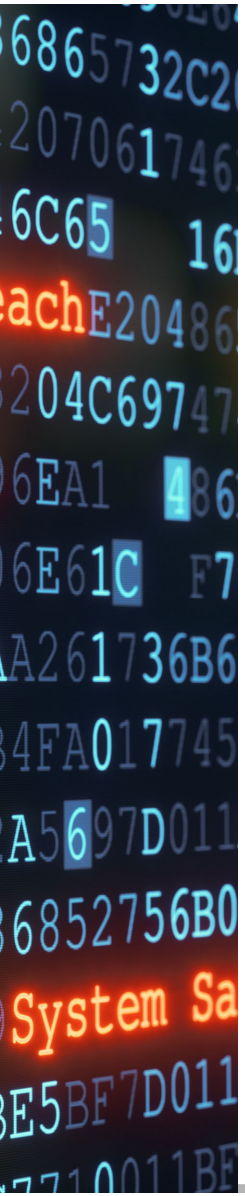
- ☐ Should report the crime to other law enforcement agencies, which may include state or local law enforcement, the Federal Bureau of Investigation (FBI), and/or the Secret Service. Any such reports should not include protected health information, unless otherwise permitted by the HIPAA Privacy Rule.[v] If a law enforcement official tells the entity that any potential breach report would impede a criminal investigation or harm national security, the entity must delay reporting a breach (see below) for the time the law enforcement official requests in writing, or for 30 days, if the request is made orally.[vi]

- ☐ Should report all cyber threat indicators[vii] to federal and information-sharing and analysis organizations (ISAOs), including the Department of Homeland Security, the HHS Assistant Secretary for Preparedness and Response, and private-sector cyber-threat ISAOs. Any such reports should not include protected health information. OCR does not receive such reports from its federal or HHS partners.[viii]

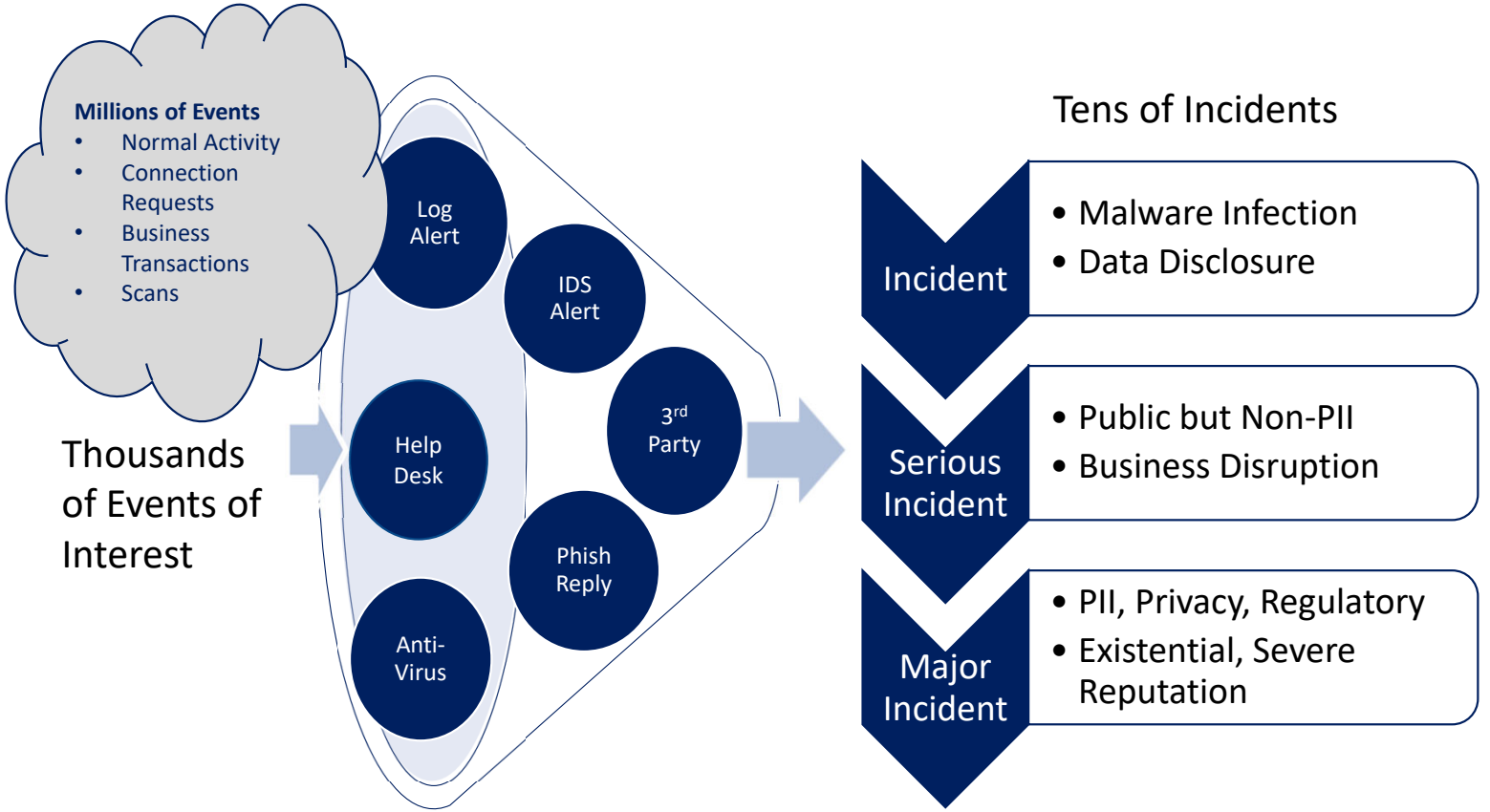
- ☐ Must report the breach[ix] to OCR as soon as possible, but no later than 60 days after the discovery of a breach affecting 500 or more individuals, and notify affected individuals and the media unless a law enforcement official has requested a delay in the reporting. OCR presumes all cyber-related security incidents where protected health information was accessed, acquired,

THE GUIDANCE





BIRTH OF A MAJOR INCIDENT



HOLLAND&HART LLP

INCIDENT HANDLING LIFECYCLE

Preparation
- Key Contact List, Test your plans (table top)
- Funding, Human Resources, Contracts in Place
- Toolkit, Written Procedures, Process, Roles & Resp.

Identification
- Events of Interest
- Incident Type
- Vitals: system, location, owner, data, pivot, etc.

Containment
- Watch & Learn or Disconnect
- Stop the bleeding, kill chains, run book
- Isolate, backup, forensic capture

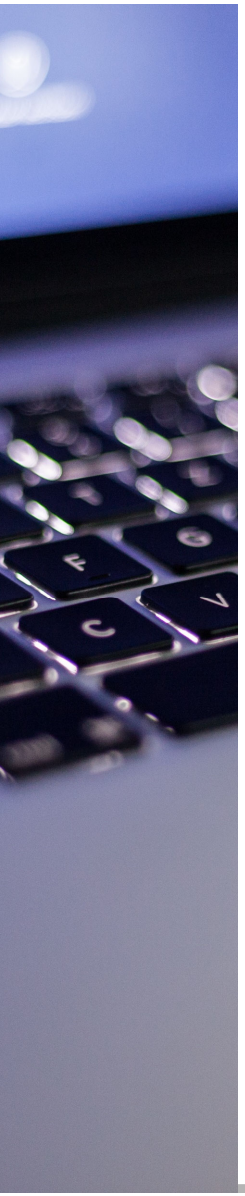
Eradication
- Close access, remove accounts
- Address vulnerability
- Clean up

Recovery
- System restore
- Test

Form Investigation Team, Including Counsel

https://www.sans.org/score/incident-forms/

https://www.sans.org/media/score/checklists/APT-IncidentHandling-Checklist.pdf



INTERNAL INVESTIGATION TEAM

Purpose:

- provide legal advice and counsel on the circumstances surrounding a data incident.

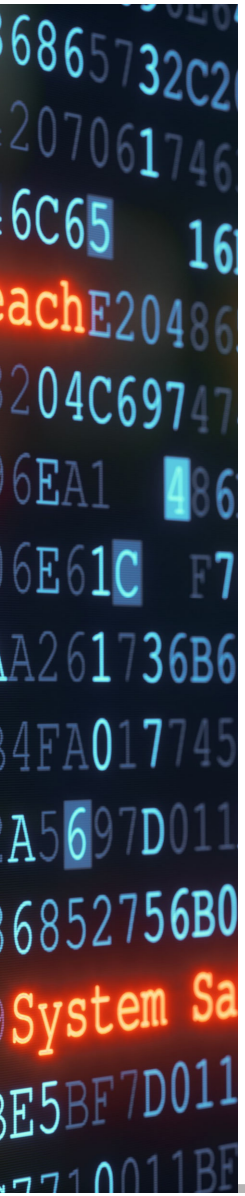
An Internal Investigation seeks to:

- ascertain relevant facts;
- determine whether violations of any applicable statutory or regulatory provisions may have occurred;
- assess remedial and mitigation measures; and
- recommend enhancements of compliance measures, if appropriate.

PRIVILEGE PROTECTION

"The attorney-client privilege is, perhaps, the most sacred of all legally recognized privileges." This applies if the communication was: (a) between attorney and client, and (b) for purposes of seeking or rendering legal advice.

The Work-Product Doctrine: "a party may not discover documents and tangible things that are prepared in anticipation of litigation or for trial"

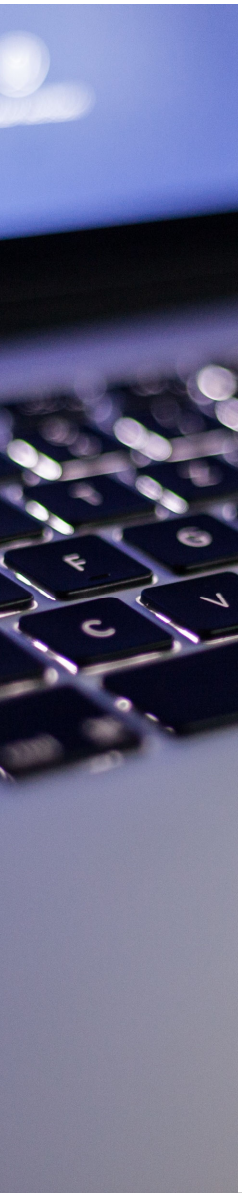


INCIDENT TRIAGE (IDENTIFICATION & VALIDATION)

- What systems are involved?
- What data is at risk?
- What are the physical locations?
- Where on the network?
- Who are the business owners of the systems and data?
- What possible pivots?

IDENTIFY WHAT HAS BEEN LOST (CONTAIN.)

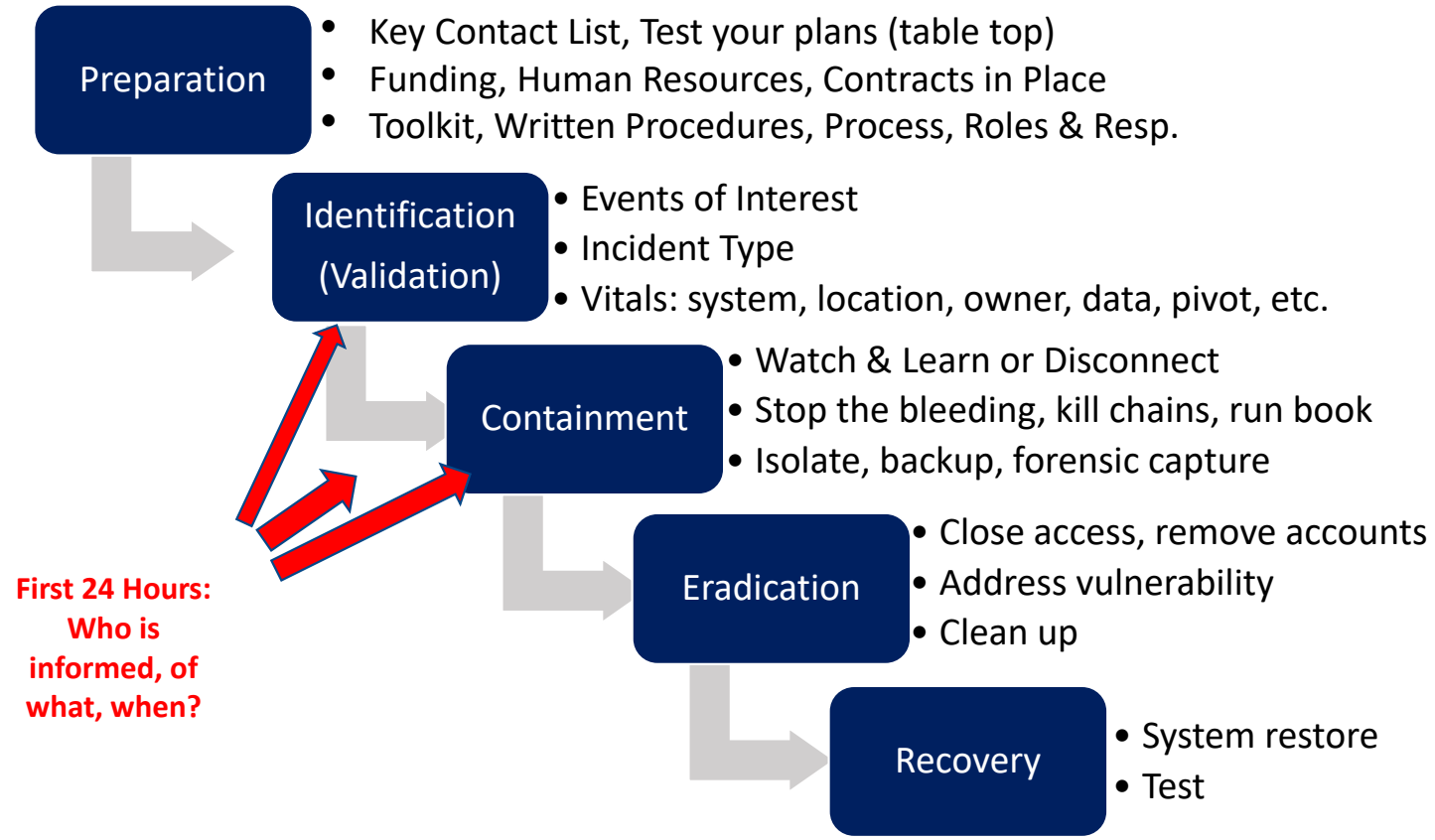
- Update NIDS/HIDS to search
- Full packet capture
- Break encrypted channels
- Host-based forensics
- Identify legal ramifications
  - International (PII, data sovereignty)
  - PCI
  - HIPAA
  - GLBA
  - SEC
  - Contractual Notifications
  - State Breach Notification
- Determine scope of notification:
  - Victims
  - Domestic and foreign regulators
  - Business partners
  - Contractual third parties
  - Public/Press



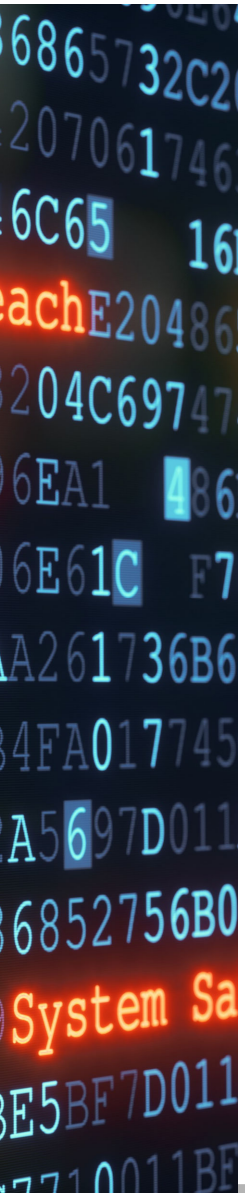
CONTAINMENT (CONT.)

- Know reasonably well before going public:
  - Incident is not ongoing
  - Type of incident
  - Size of breach
  - Medium of data: hard copy, electronic or both?
  - Location, jurisdictions and controlling law
  - Timing of incident:
    - First discovered
    - Internal communications
  - Data affected, elements compromised

INCIDENT HANDLING LIFECYCLE

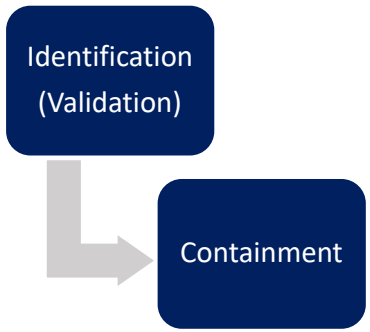


https://www.sans.org/score/incident-forms/
https://www.sans.org/media/score/checklists/APT-IncidentHandling-Checklist.pdf



INTERNAL COMMUNICATIONS (IDENTIFICATION)

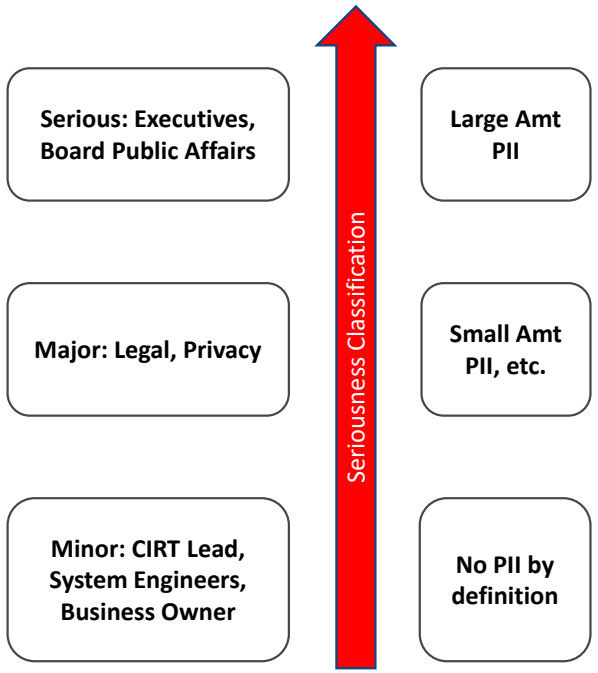
- Validate suspected incident first!
- Incident classification determines stakeholders (Minor, Serious, Major)
- Don't raise false alarms
- When to notify (by Incident Response Phase):

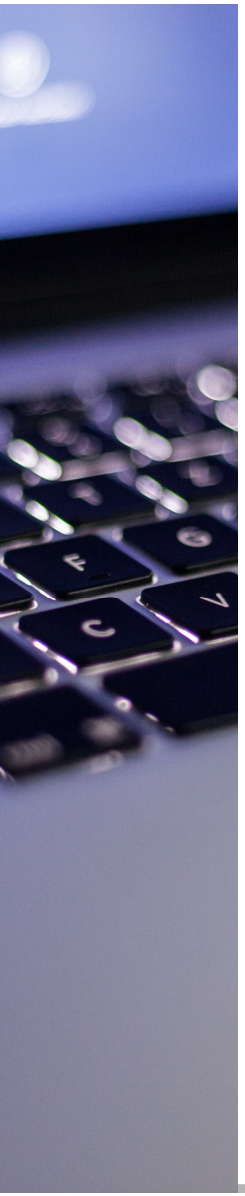


- <u>Upon Identification</u>
  - Notify IRT Lead
- <u>Upon Validation</u>, Notify:
  - Minor: System Owner, Engineers
  - Minor: CISO, Affected Business Line
  - Serious: General Counsel, Compliance, Privacy
  - Major: Executives, Board
  - Major: Insurance Broker
- <u>Upon Containment</u>:
  - Serious/Major: Forensics Team

INTERNAL COMMUNICATIONS

- Benefits of Involving Legal Early (Upon Incident Validation, Serious or Major)
  - Formation of Incident Investigation Team
  - Communications Limited to Team Members
  - Protects Attorney-Client Privilege
    - Include outside counsel as party to service contracts for forensics, security consulting, etc.
  - Protect Information About WHY the Incident Happened; subject of future litigation, regulatory inquiry



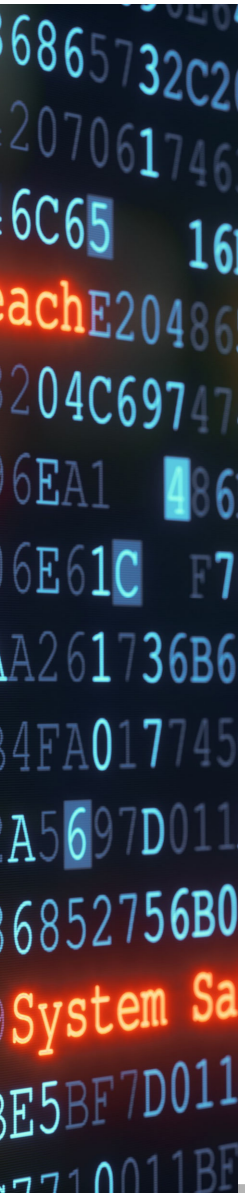


KEY CONTACT LIST

- Corporate Security Officer or CISO
- CIRT, CSIRT, Incident Handling Team (in house or contract)
- Corporate Legal Officer
- Outside Data Security or Privacy Counsel
- Insurance Agent
- CIO or Systems Manager
- Privacy Officer
- Public Affairs/Corp. Comm.
- ISP Technical Contact
- Local FBI Field Office
- Local Law Enforcement Computer Crime
- Key Vendor Contacts (Software, Infrastructure, Data Center)
- Local Computer Forensics Contractor (funded, contracted)
- Optional:
  - Malware Reverse Engineering Contractor (funded, contracted)

NOTIFICATION (CONTAINMENT)

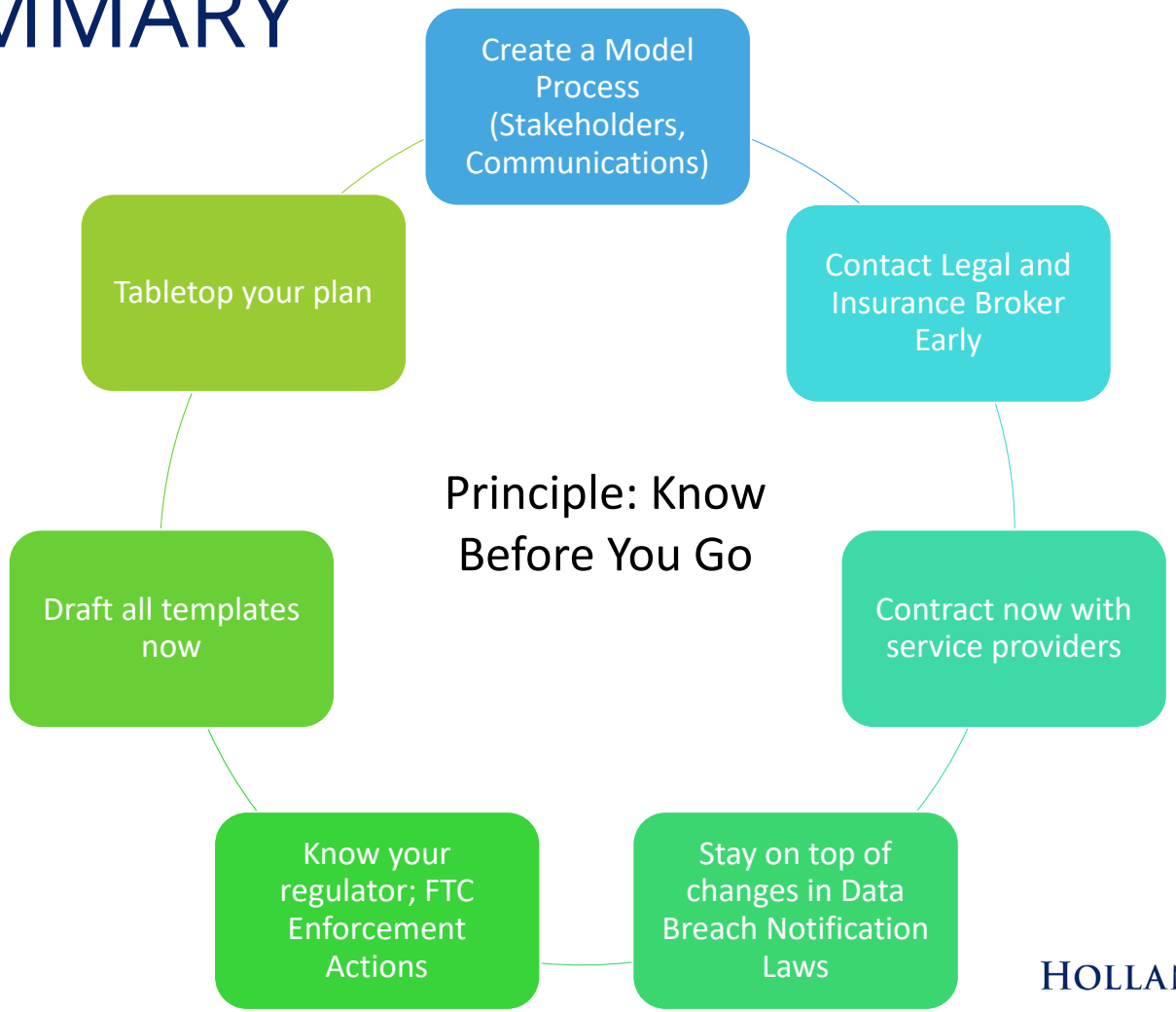
- Do not go public prematurely
- Maintain an expedient internal investigation, do not delay
- Facts are needed, they come as investigation progresses
- Multiple notifications as facts arrive are viewed suspiciously, convey sense of uncertainty, frustration among victims
- However, all delays must be justified



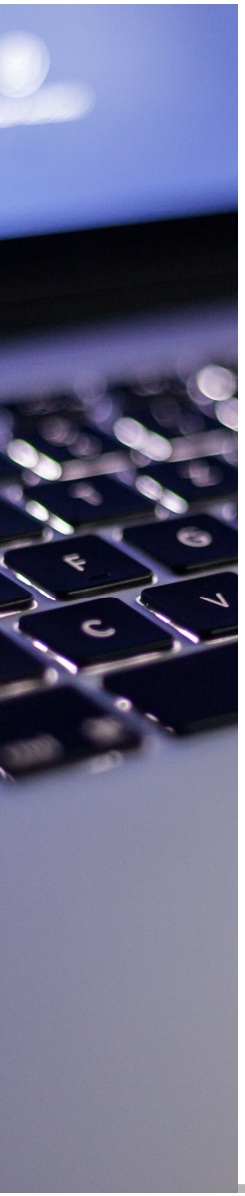
ERADICATION

- Capture evidence of wrong doing
- Forensically image impacted disk drives, replace with clean installs
- Maintain chain of custody on all drives and forensic images
- Use working copies for analysis while preserving original drives
- Advanced attacks are only discovered in RAM, do not write to drive
- Close all outbound data exfiltration channels
- Close and patch all vulnerabilities

SUMMARY



HOLLAND&HART LLP



ACTION PLAN

When you get back to your office

- Inquire about your incident response plan, review it
- Call a stakeholder meeting to plan improvements to breach readiness

In the first 30 days

- Update incident response plan
- Update key contacts
- Initiate review of data breach notification requirements (state, federal, intl., contractual)

By 90 days

- Draft all templates
- Identify and source external service providers
- Finalize roles & responsibilities

End of year

- Complete table top exercise
- Complete post-mortem on all incidents
- Improve security program to prevent incidents (CSF and 20CC)

ACTION PLAN

When you return to work:

- Identify when your next risk assessment is due
- Review last risk assessment
- Identify shortcomings

30 days:

- Discuss noted shortcomings with management
- Assign accountable party to plan for upcoming risk assessment to address observed weaknesses, based on OCR guidance

90 days:

- Complete inventory of: ePHI, storage media, transmission, systems and endpoints

180 days:

- Conduct an improved risk assessment

NACD – 5 KEY OVERSIGHT STEPS

Understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue

Understand the legal implications of cyber security risks as they relate to their company's specific circumstances

Board members should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the meeting agenda

Set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget

Discussions of cyber-risk should include identification of what risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach

ACTION ITEMS FOR DIRECTORS

- Facilitate a culture that views cybersecurity as a business issue that all employees should understand and participate in. As part of that, companies should consider employee training and awareness programs;
- Include a cyber-expert on the company's board of directors or receive regulator reports from a cybersecurity expert that are discussed at board meetings;
- Ensure the company has an updated plan to respond to a cybersecurity attack, should it experience one. As part of that, senior management should become familiar with the legal and contractual requirements to determine what steps they would be required to take if the company fell victim to a data breach;
- Ensure that the applicable directors and officers' insurance covers data breach lawsuits, and
- Directors may consider the guidance provided by the Cybersecurity Framework released in February by the National Institute of Standards and Technology in response to U.S. President Barack Obama's Executive Order 13636, which was intended to be used by companies to create a cybersecurity program.

HOLLAND&HART LLP

THANK YOU!

RICH SPILDE

rdspilde@hollandhart.com

303.473.4808

HOLLAND&HART LLP