



CYBERSECURITY

2019 Wyoming Healthcare Compliance Bootcamp
Cheyenne Regional Medical Center
Friday, November 8, 2019

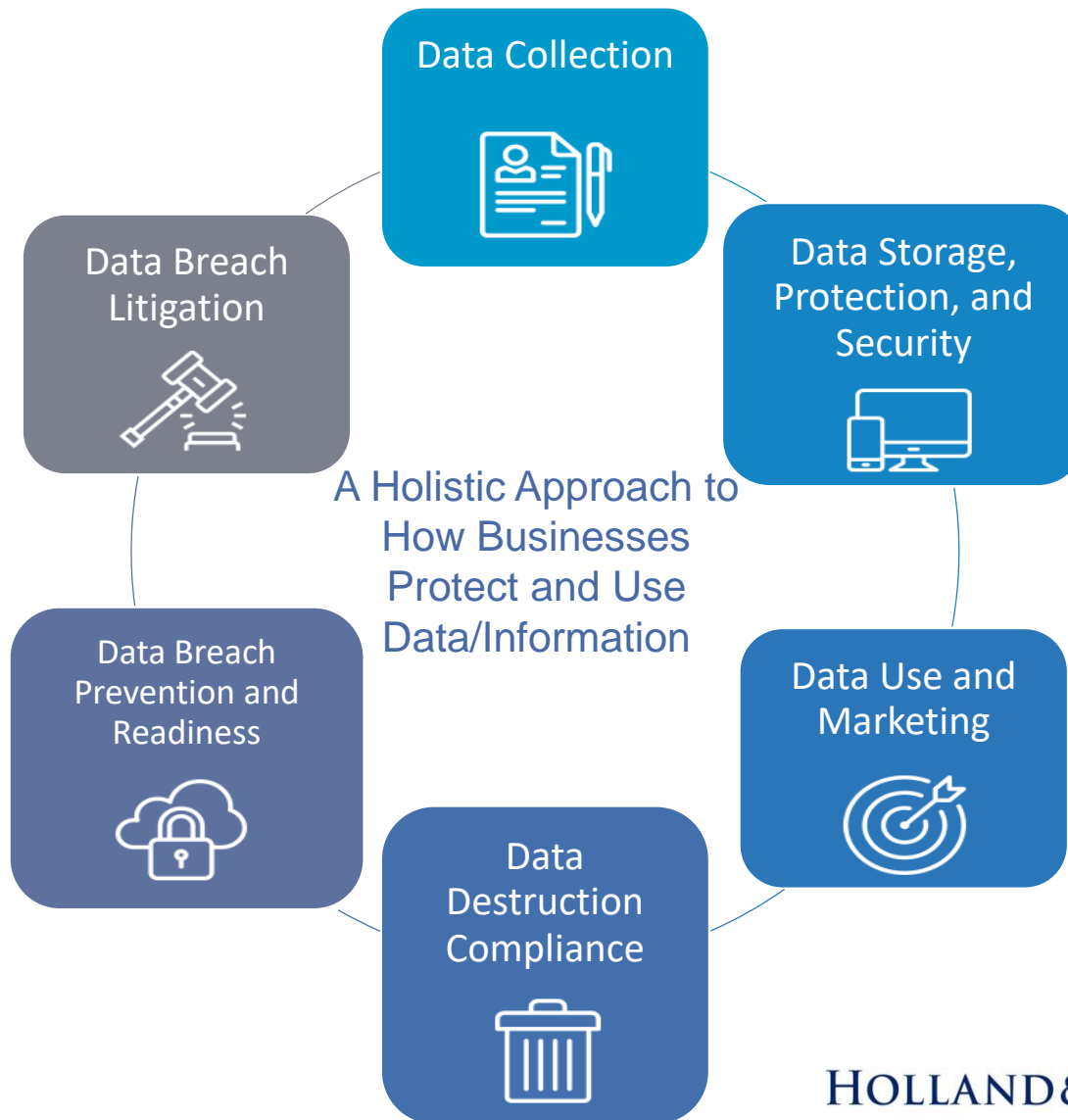
A decorative graphic at the top of the slide featuring a network of glowing blue lines and nodes, resembling a molecular structure or a digital network, set against a dark blue background.

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.

All Presentations and Other Materials © Holland & Hart LLP
2019

THE DATA LIFECYCLE





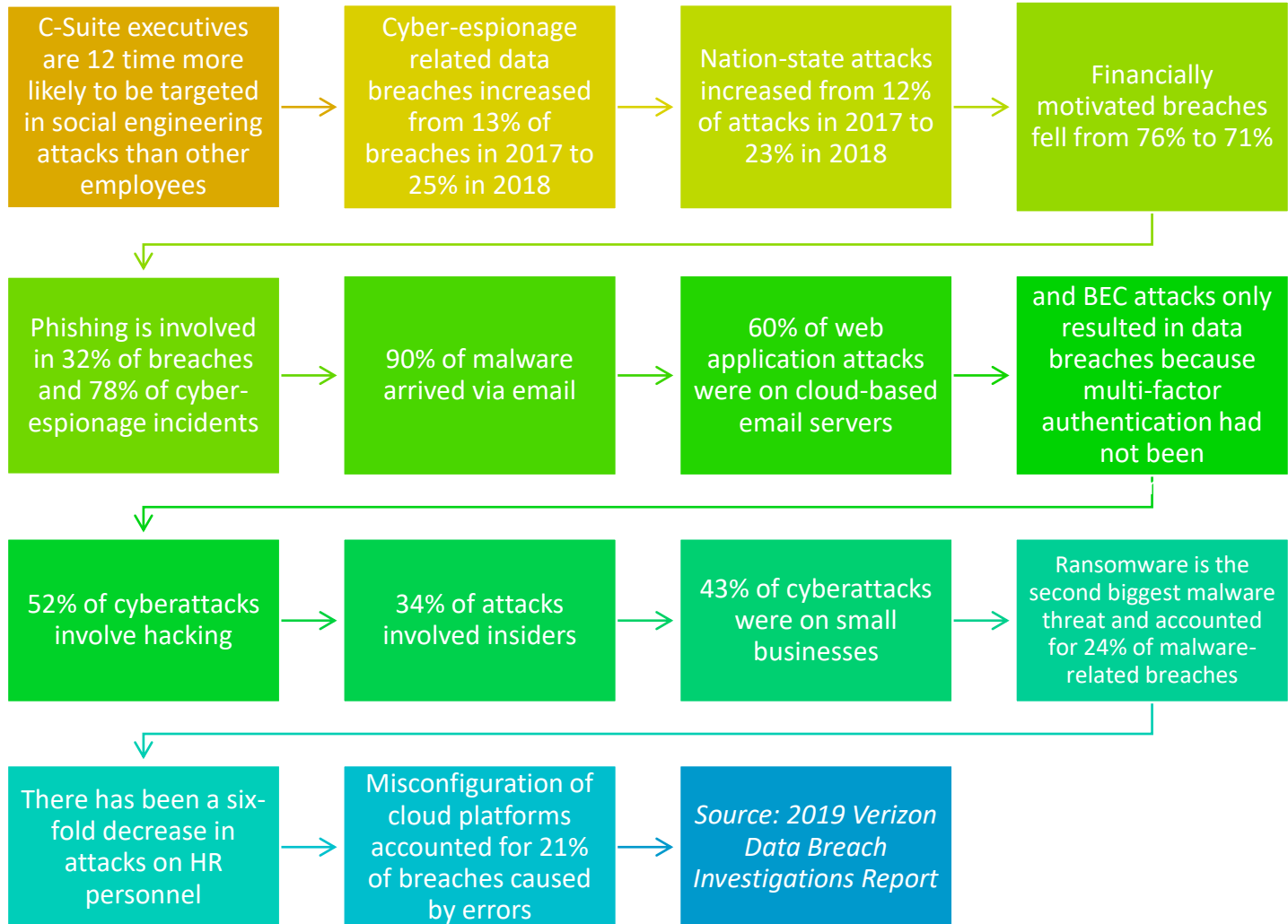
THE AGENDA

The Threats

The Guidance

The Breach

2019 VERIZON DATA BREACH STUDY



VERIZON DATA BREACH STUDY

- Out of all industry sectors analyzed, healthcare was the only industry where the number of incidents caused by insiders was greater than those caused by external threat actors. 59% of incidents involved insiders compared to 42% involving external threat actors. Breaches of medical information are 14 times more likely to be caused by doctors and nurses.
- The primary motive for attacks on the healthcare industry was financial gain (83%), followed by fun (6%), convenience (3%), because a grudge was held (3%), and espionage (2%). 72% of breaches involved medical data, 34% involved personal information, and 25% involved credential theft.
- 81% of all healthcare cybersecurity incidents involved either miscellaneous errors such as software misconfiguration, privilege misuse, and web applications.
- *Source: 2019 Verizon Data Breach Investigations Report*

2019 VERIZON DATA BREACH STUDY

Pattern	Number of Data Breaches
Miscellaneous Errors	97
Privilege Misuse	85
Web Applications	65
Lost and Stolen Assets	28
Everything Else	27
Cyber-Espionage	2
Point of Sale	2
Crimeware	1
Denial of Service	0

HALLOWEEN MAY BE OVER, BUT . . .

- In 2018, the healthcare sector saw 15 million patient records compromised in 503 breaches, three times the amount seen in 2017, according to the Protenus Breach Barometer. But just over halfway through 2019, and the numbers have skyrocketed with potentially more than 25 million patient records breached.
- Healthcare has been peppered with massive data breaches, with each of the 10 largest seeing more than 200,000 records breached at a time. What's worse is that many of these went on for extended periods of time, while others failed to report within the HIPAA-mandated **60 days**.
- Third-party vendors and phishing attacks were behind most of these security incidents, and the investigations into the largest vendor breach is still ongoing. As it stands, 2019 may prove to be the worst seen for healthcare cybersecurity.





THE HEALTHCARE TOP 10

AMCA DATA BREACH: 25 MILLION PATIENTS, INVESTIGATIONS ONGOING

In early May, an 8-K filing with the Securities and Exchange Commission revealed billing services vendor American Medical Collection Agency was hacked for eight months between August 1, 2018 and March 30, 2019. Since the breach was revealed, at least six covered entities have come forward to report their patient data was compromised by the hack. However, the majority of the impacted providers are still continuing to investigate the scope of the breach, so the total amount of affected patients will be unclear into the foreseeable future.

AMCA's parent company has since filed bankruptcy, while the billing services vendor, Quest and LabCorp are facing numerous investigations and lawsuits.

DOMINION NATIONAL: 2.96 MILLION PATIENTS

Insurer Dominion National reported *a nine-year hack on its servers*, which potentially breached the data of 2.96 million patients. An internal alert revealed unauthorized access on its systems, which prompted an investigation. Officials said they found the unauthorized access began as early as August 25, 2010, nearly nine years before the breach was discovered in April 2019.

INMEDIATA HEALTH GROUP: 1.5 MILLION PATIENTS

A misconfigured database led to a personal health data breach of 1.57 million Inmediata Health Group patients. What's worse: the provider inadvertently mailed patients the wrong letters during the breach notification process.

The compromised database was discovered in January, when officials found a search engine function was allowing internal Inmediata webpages used for business operations to be indexed. As a result, some electronic health information was exposed.

THE HEALTHCARE TOP 10

UW MEDICINE: 973,024 PATIENTS

In February, the University of Washington Medicine began notifying 974,000 patients that their data was exposed online for three weeks due to a ***misconfigured server***. The breach was discovered in December 2018 when a patient conducted a search of their own name and found a file containing their personal information. They notified UW Medicine, which determined an employee error three weeks prior caused internal files to become publicly accessible.

WOLVERINE SOLUTIONS GROUP: ESTIMATED 600,000 PATIENTS

While the Wolverine Solutions Group ransomware attack occurred in September 2018, the third-party vendor performed “rolling notifications” to its impacted healthcare clients. As a result, some providers received notifications as late as March 2019. ***WSG systems were infected with ransomware*** in September, and decryption and file restoration continued throughout October. The cyberattack potentially compromised a wide range of data from a host of clients, including demographic details and Social Security numbers.

OREGON DEPARTMENT OF HUMAN SERVICES: 645,000 PATIENTS

Initially announced in March, Oregon Department of Human Services began notifying additional patients in June of a breach caused by a ***massive phishing campaign***. In total, 625,000 patients and 2.5 million emails were compromised. In January, a targeted phishing attack caused nine employees to respond to the malicious emails and provide their user credentials. As a result, hackers gained full access to their email accounts, messages and attachments. It took Oregon DHS officials three weeks to discover the hack, when those employees reported account issues to the security team.



THE HEALTHCARE TOP 10

COLUMBIA SURGICAL SPECIALIST OF SPOKANE: 400,000 PATIENTS

Details into the Columbia Surgical Specialist of Spokane breach are limited. But according to the HHS breach reporting tool, the Washington provider reported a **hacking incident in February impacting 400,000 patients**.

There's no public notice on the specialist's site, but reportedly it was a ransomware attack that began on January 7. Columbia Surgical Specialist did not pay the ransom and restored data from backups.

UCONN HEALTH: 326,629 PATIENTS

The personal and health data of about 326,629 UConn Health patients was potentially breached after several employees **fell victim to phishing attacks** in December. In February, UConn Health discovered a hacker accessed a number of employee email accounts and immediately secured the accounts.

NAVICENT HEALTH: 278,016 PATIENTS

An unauthorized third-party gained access to Navicent Health employee and hosted email accounts in July 2018, which potentially breached the data of 278,016 patients.

An investigation was launched into the security incident, which concluded on January 24. Navicent Health began notifying patients in March, eight months after the breach. HIPAA requires providers to notify patients of a breach within 60 days.

ZOLL SERVICES: 277,319 PATIENTS

Medical device vendor ZOLL Services notified 277,319 patients in March of a breach to their personal and medical data, **caused by a server migration error**. On January 24, officials found some emails archived by its third-party service vendor exposed during a routine server migration. The vendor was tasked with record retention and maintenance requirements.

THE GUIDANCE

y/guidance/cybersecurity/index.html

HHS.gov U.S. Department of Health & Human Services
Health Information Privacy

I'm looking for...  [HHS A-Z Index](#)

 **HIPAA for Individuals**  **Filing a Complaint**  **HIPAA for Professionals**  **Newsroom**

[HHS](#) > [HIPAA Home](#) > [For Professionals](#) > [Security](#) > [Guidance](#) > Cyber Security Guidance Material

Text Resize [A](#) [A](#) [A](#) Print  Share   

HIPAA for Professionals

Regulatory Initiatives

Privacy +

Security -

- Summary of the Security Rule
- Guidance
- Cyber Security Guidance

Breach Notification +

Compliance & Enforcement +

Special Topics +

Patient Safety +

Covered Entities & Business Associates +

Cyber Security Guidance Material

In this section, you will find educational materials specifically designed to give HIPAA covered entities and business associates insight into how to respond to a cyber-related security incidents.

Cyber Security Checklist and Infographic

This guide and graphic explains, in brief, the steps for a HIPAA covered entity or its business associate to take in response to a cyber-related security incident.

[Cyber Security Checklist - PDF](#)

[Cyber Security Infographic](#) [GIF 802 KB]

Ransomware Guidance

HHS has developed guidance to help covered entities and business associates better understand and respond to the threat of ransomware.

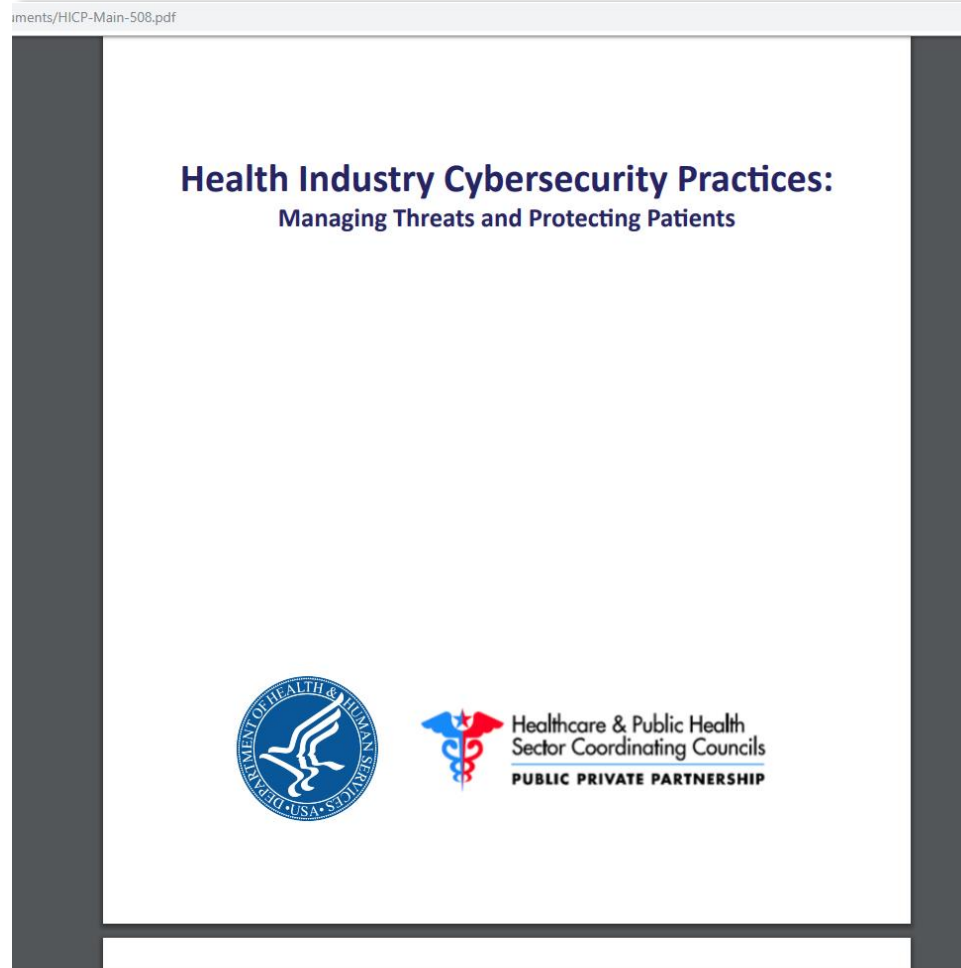
[Ransomware - PDF](#)

National Institute of Standards and Technology (NIST) Cybersecurity Framework

This crosswalk document identifies "mappings" between NIST's Framework for Improving Critical Infrastructure Cybersecurity and the HIPAA Security Rule.

[NIST Cyber Security Framework to HIPAA Security Rule Crosswalk - PDF](#)

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”*



2019 5 MOST 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.



THREAT: E-MAIL PHISHING ATTACK

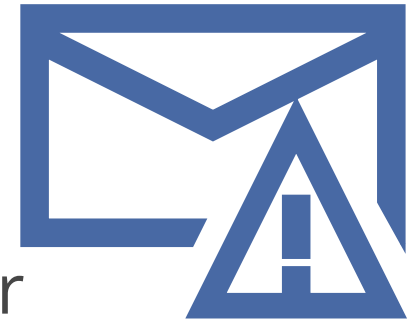
- On average, a person will receive about 80 e-mails per day. Knowing which are safe to open can get tricky if you are not asking yourself the following questions:
 - Do you know the sender?
 - Are there any spelling or grammatical errors, or any other indicators that the tone or style of the e-mail is off?
 - Before clicking on a link, did you hover over it to see the URL destination?
 - Do you know the sender, or are you suspicious of the e-mail? If in doubt, do NOT open any attachments.
 - What are my organization's processes for reporting suspicious e-mails?
- The best time to familiarize yourself with your organization's policies for reporting a suspicious e-mail is when you begin employment. Whenever you receive an e-mail that sounds too good to be true or that you were not expecting, verify it before opening it!
- Check with colleagues to find out whether they received the same phishy e-mail. You can always seek the guidance of your IT security support team or similar point of contact. Talk to them to find out whether your account is protected with the proper security filters to ward off unwanted junk mail.

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.



THREAT: 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)

THREAT: RANSOMWARE ATTACK

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)

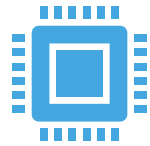
Once ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures (HHS Ransomware Fact Sheet)

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



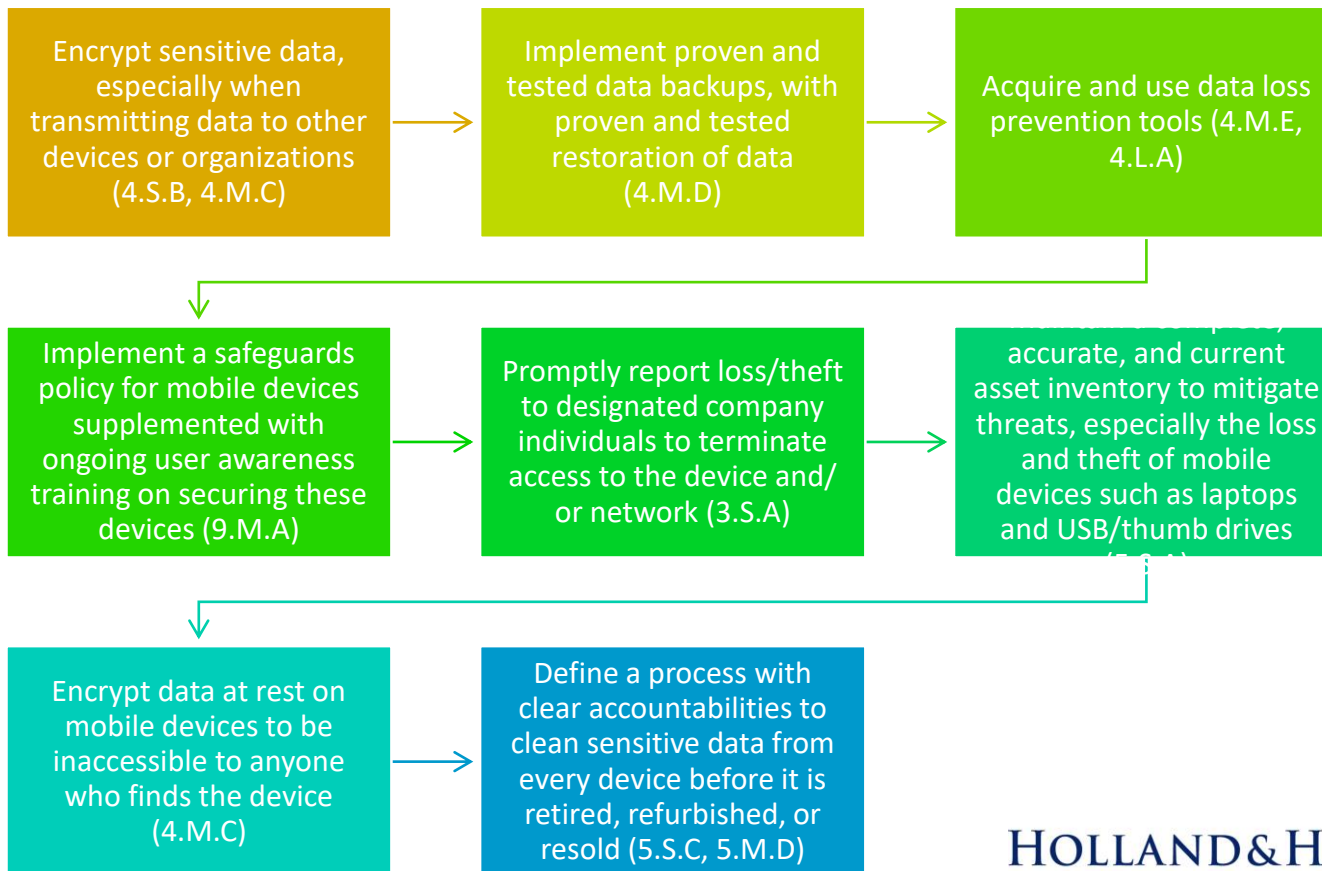
Heading out on a business trip or a personal holiday? You need to follow the same, and maybe greater, security procedures as you do in the office. Make sure you know your organization's policy on removing equipment from the workplace by asking:

- 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, password protected 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.

THREAT: LOSS OR THEFT OF EQUIPMENT OR DATA



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.



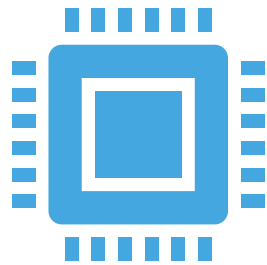
Always consult your IT security professionals when exposed to a situation of stolen data or employee misconduct. Every situation will vary so your IT security professionals will be able to guide you best because a cyber-threat is not limited to hacking.



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 PERSONAL SAFETY

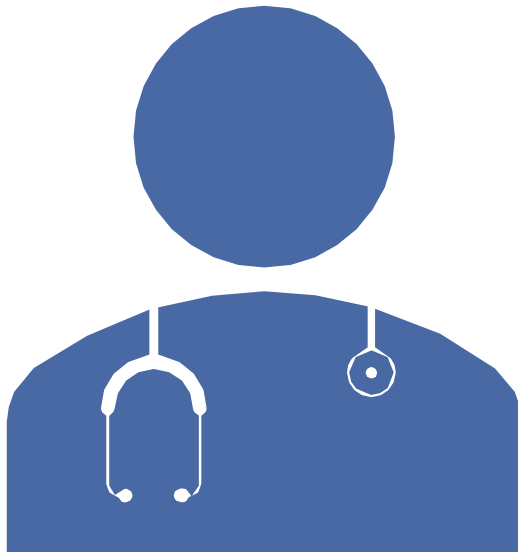


Real-World Scenario: A cyber attacker gains access to a care provider's computer network through an e-mail phishing attack and takes command of a file server to which a heart monitor is attached. While scanning the network for devices, the attacker takes control (e.g., power off, continuously reboot)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



THREAT: ATTACKS AGAINST CONNECTED MEDICAL DEVICES THAT MAY AFFECT PERSONAL 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 do we notify patients if their medical devices are compromised? • How do patients 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 your 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, and appropriate protection and response measures.

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

- Establish and maintain communication with medical device manufacturer's product security 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 Control (MAC) address, Internet Protocol (IP) address, network segments, operating systems, applications, and other elements relevant to managing information security risks (9.M.D)
- Implement pre-procurement security requirements for vendors (9.L.C)
- Implement information security assurance practices, such as security risk assessments of 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.L.C)
- Implement access controls for clinical and vendor support staff, including remote access, 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 networks (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)
Evaluation	164.308(a)(8)	Applications and Data Criticality Analysis (A) (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 Workstation Use Workstation Security Device and Media Controls	164.310(a)(1) 164.310(b) 164.310(c) 164.310(d)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A) (R) (R) 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

<https://www.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

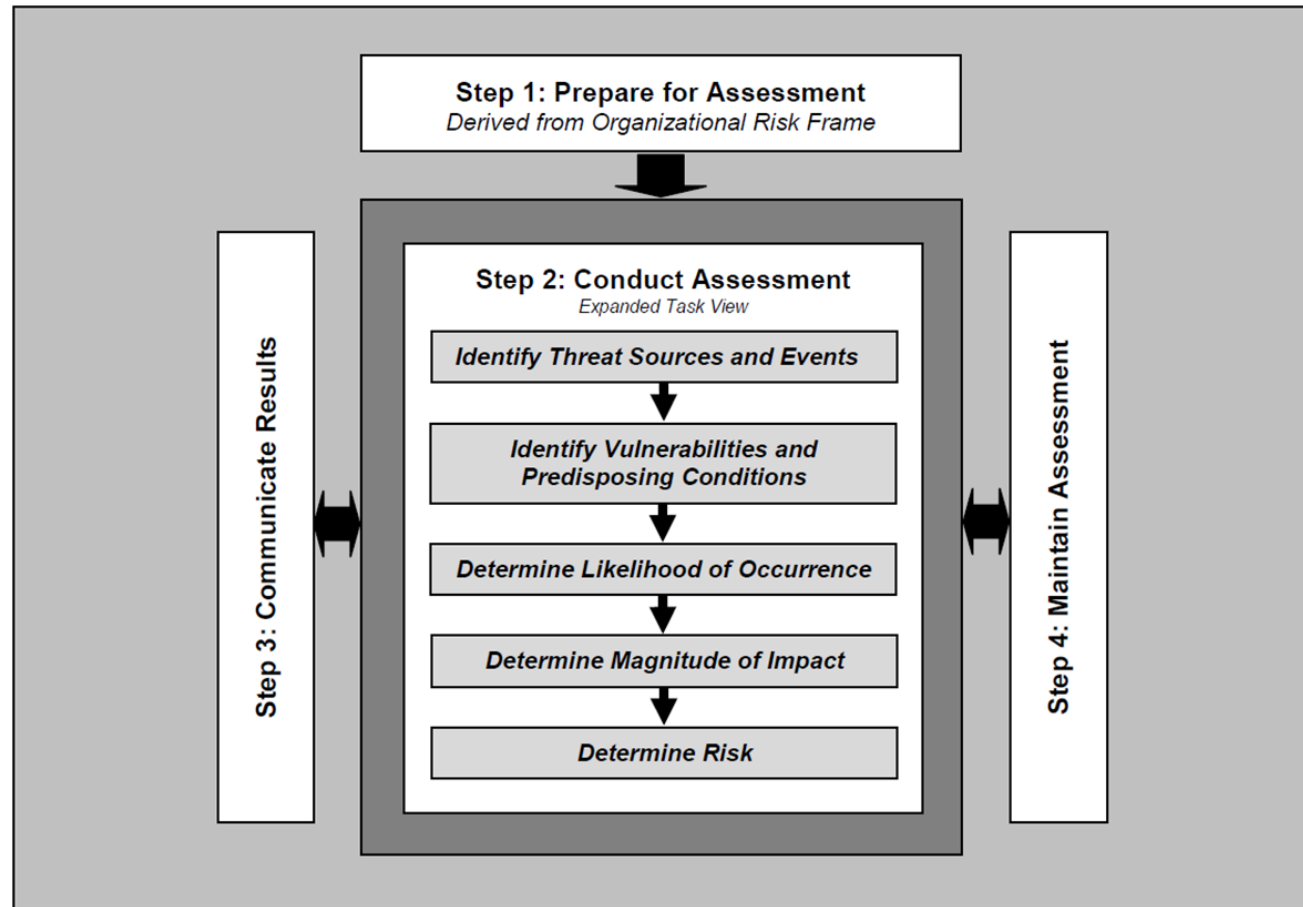


FIGURE 5: RISK ASSESSMENT PROCESS

HHS RISK ASSESSMENT TOOL

/privacy-security-and-hipaa/security-risk-assessment-tool

CONTACT | EMAIL UPDATES

HealthIT.gov Official Website of The Office of the National Coordinator for Health Information Technology (ONC)

Connect with us: [in](#) [t](#) [v](#) [r](#)

TOPICS | HOW DO I? | BLOG | NEWS | ABOUT ONC

Search

Home > Topics > Privacy, Security, and HIPAA > Security Risk Assessment Tool

Privacy, Security, and HIPAA

- Educational Videos
 - Security Risk Assessment Tool**
 - Security Risk Assessment Videos
 - Top 10 Myths of Security Risk Analysis
- HIPAA Basics
- Privacy & Security Resources & Tools
- Privacy & Security Training Games
- Model Privacy Notice (MPN)
- How APIs in Health Care can Support Access to Health Information: Learning Module
- Patient Consent and Interoperability
- Your Mobile Device and Health Information Privacy and Security

Security Risk Assessment Tool

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that covered entities and its business associates conduct a risk assessment of their healthcare organization. A risk assessment helps your organization ensure it is compliant with HIPAA's administrative, physical, and technical safeguards. A risk assessment also helps reveal areas where your organization's protected health information (PHI) could be at risk. To learn more about the assessment process and how it benefits your organization, visit the [Office for Civil Rights' official guidance](#).

What is the Security Risk Assessment Tool (SRA Tool)?

The Office of the National Coordinator for Health Information Technology (ONC), in collaboration with the HHS Office for Civil Rights (OCR), developed a downloadable Security Risk Assessment (SRA) Tool to help guide you through the process. The tool is designed to help healthcare providers conduct a security risk assessment as required by the HIPAA Security Rule and the Centers for Medicare and Medicaid Service (CMS) Electronic Health Record (EHR) Incentive Program.

[Download Version 3.1 of the SRA Tool \[msi - 102.6 MB\]](#)

All information entered into the SRA Tool is stored locally to the users' computer or tablet. HHS does not receive, collect, view, store or transmit any information entered in the SRA Tool. The results of the assessment are displayed in a report which can be used to determine risks in policies, processes and systems and methods to mitigate weaknesses are provided as the user is performing the assessment. The target audience of this tool is medium and small providers; thus, use of this tool may not be appropriate for larger organizations.

SRA Tool Update

The updated version of the popular Security Risk Assessment (SRA) Tool was released in October 2018 to make it easier to use and apply more broadly to the risks of the confidentiality, integrity, and availability of health information. The tool diagrams HIPAA Security Rule safeguards and provides enhanced functionality to document how your organization implements safeguards to mitigate, or plans to mitigate, identified risks. The new SRA Tool is available for Windows computers and laptops. However, the previous iPad version of the SRA Tool is still available from the [Apple App Store](#) (search under "HHS SRA Tool"). The SRA tool is not available for Mac OS.

The tool is now more user friendly, with helpful new features like:

- Enhanced user interface

Need Help?

Please leave any questions, comments, or feedback about the SRA Tool using our [Health IT Feedback Form](#). This includes any trouble in using the tool or problems/bugs with the application itself. Also, please feel free to leave any suggestions on how we could improve the tool in the future.


You may also leave a message with our Help Desk by contacting 734-302-4717

[Submit Questions Or Feedback](#)

SRA Webinars

ONC held 3 webinars with a training session and overview of the Security Risk Assessment (SRA) Tool. The slides for these sessions are posted below and a recording of the webinar is also available.

- [Presentation Slides \[PDF - 2MB\]](#)





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?”

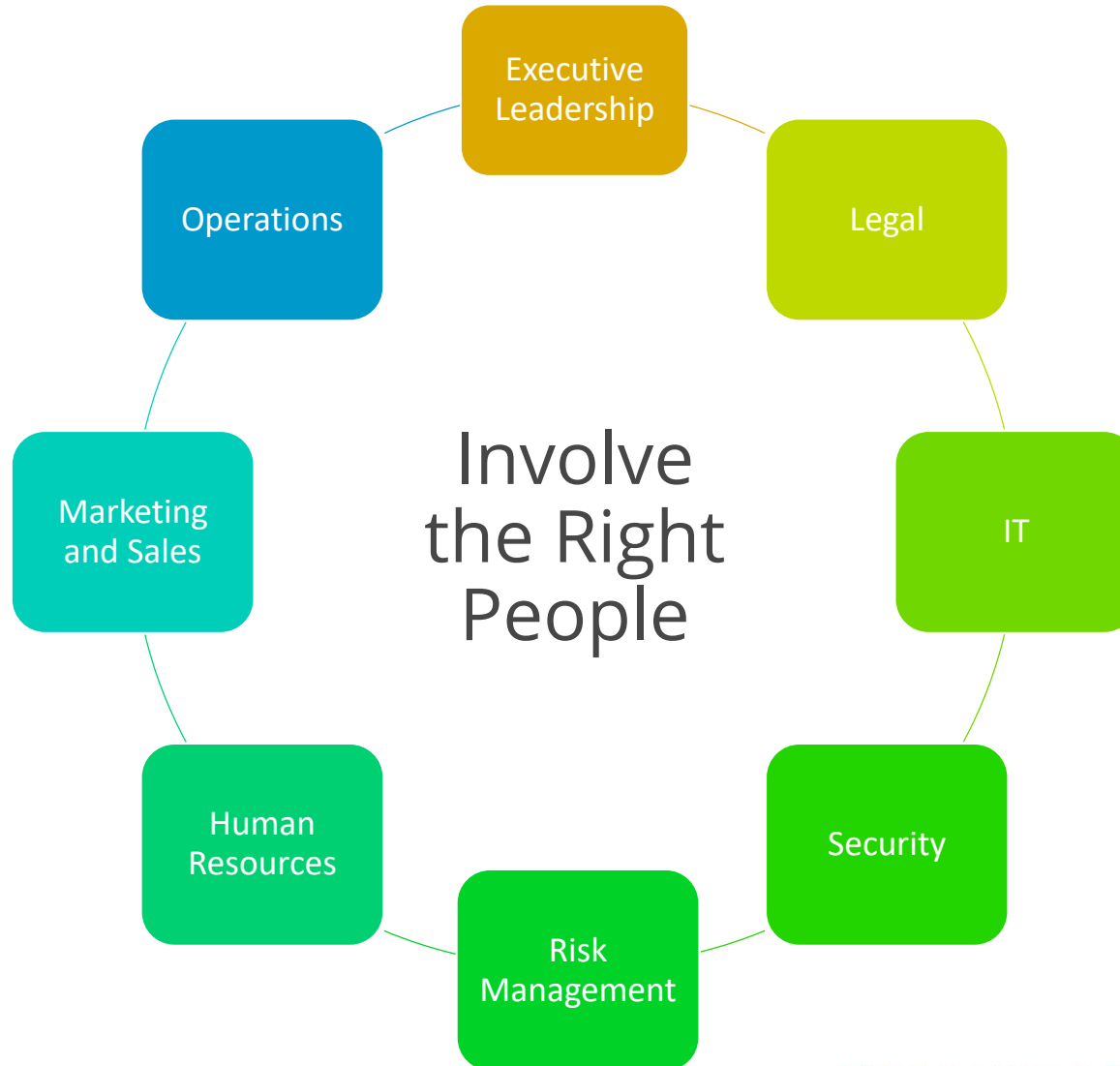
- Who can access data?
- How can they access it?
- What are the business needs for accessing it?

What are your policies, procedures and rules?

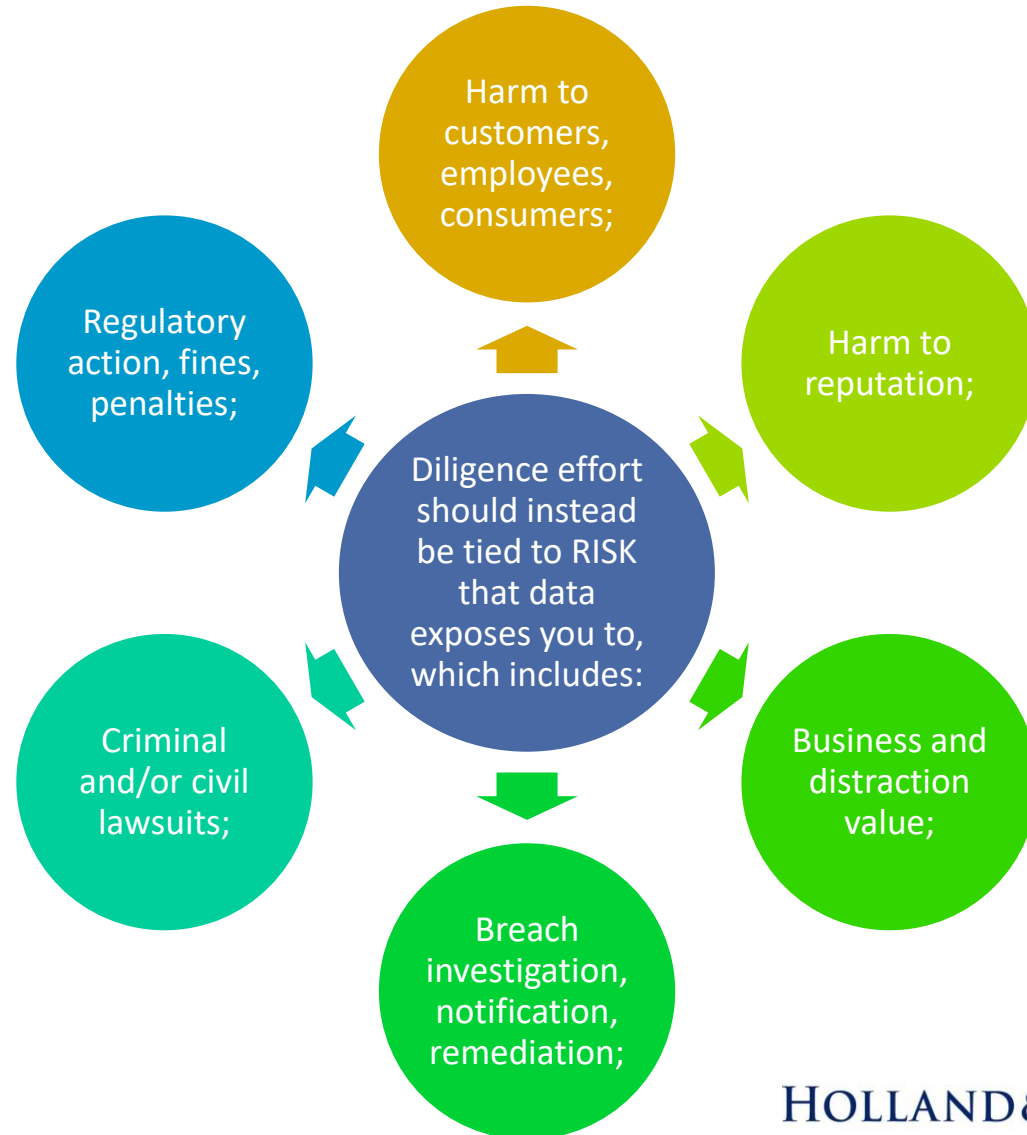
What do you need to be compliant with, and are you?

What security methodology and standards do you follow?

INTERNAL DILIGENCE



EFFORT LEVEL = RISK LEVEL



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

06-2017.pdf



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

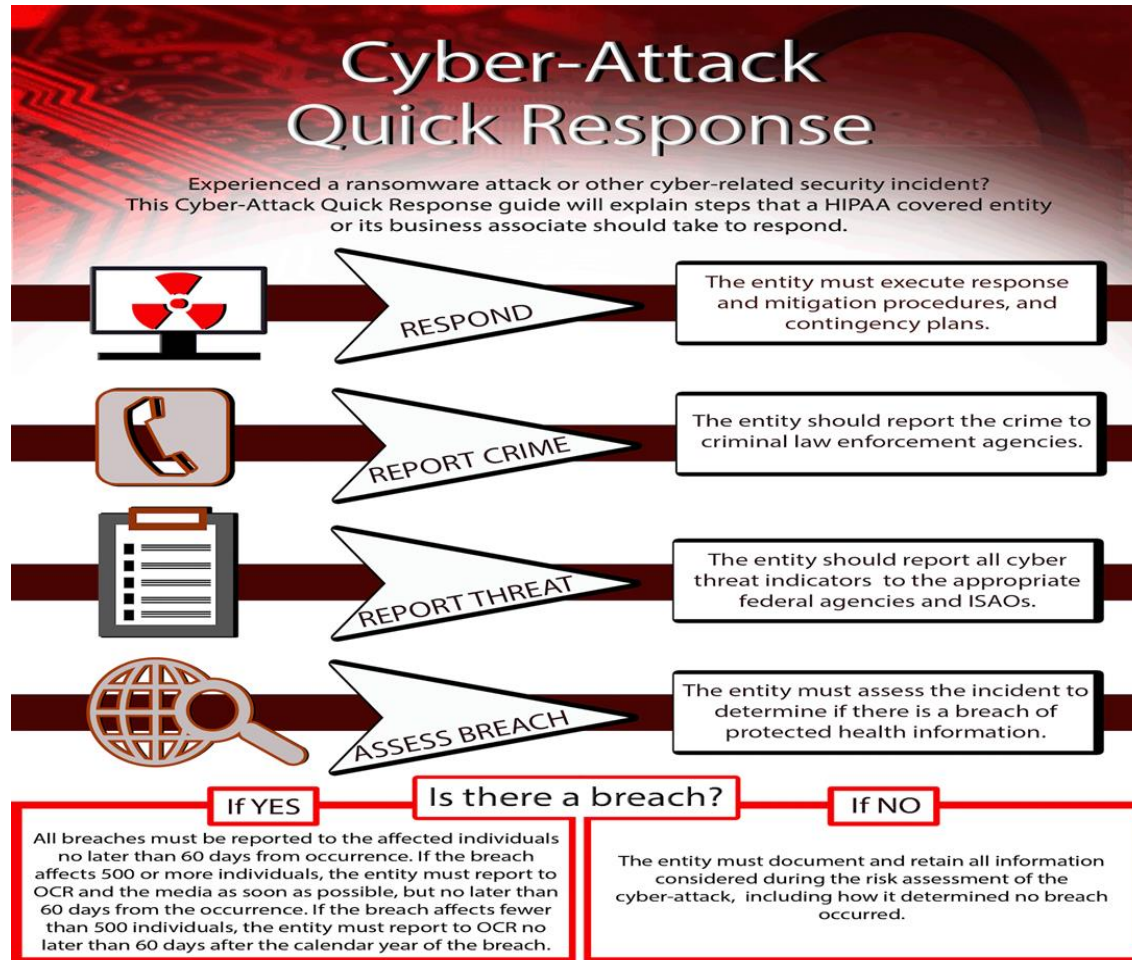
My entity just experienced a cyber-attack! What do we do now?

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

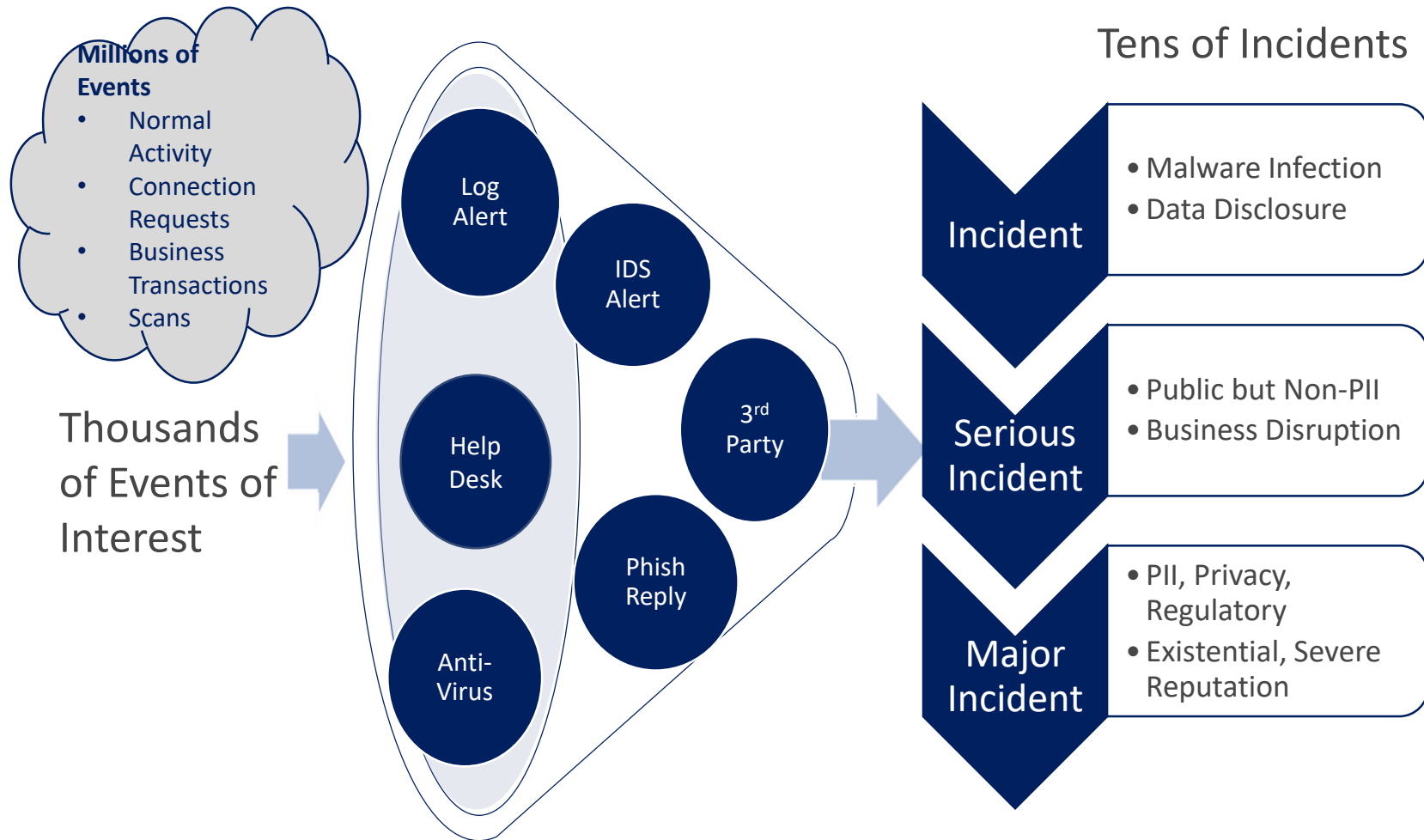
Has your entity just experienced a ransomware attack or other cyber-related security incident,ⁱ and you are wondering what to do now? This guide explains, in brief, the steps for a HIPAA covered entity or its business associate (the entity) to take in response to a cyber-related security incident. In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

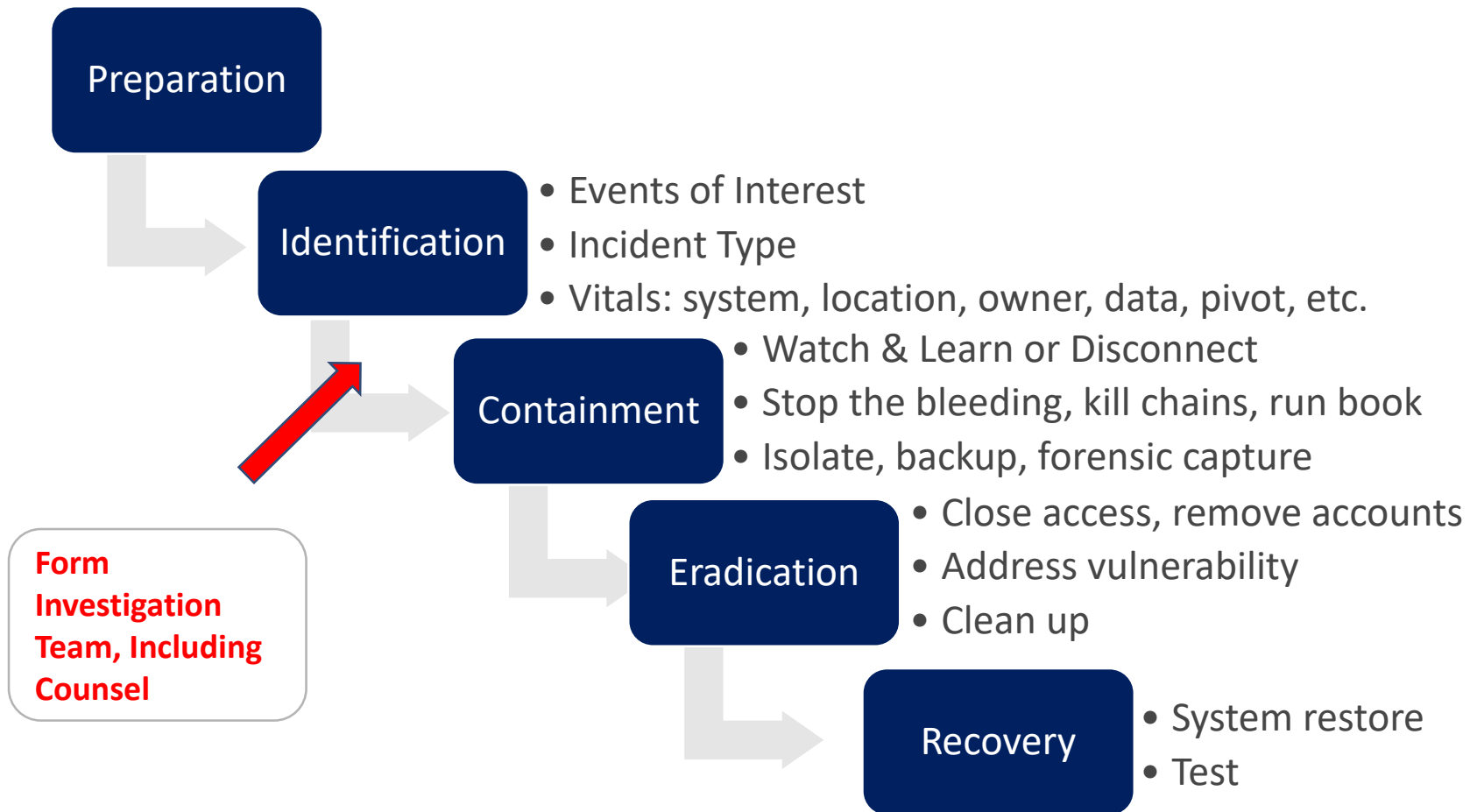
THE GUIDANCE



BIRTH OF A MAJOR INCIDENT



INCIDENT HANDLING LIFECYCLE



<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?

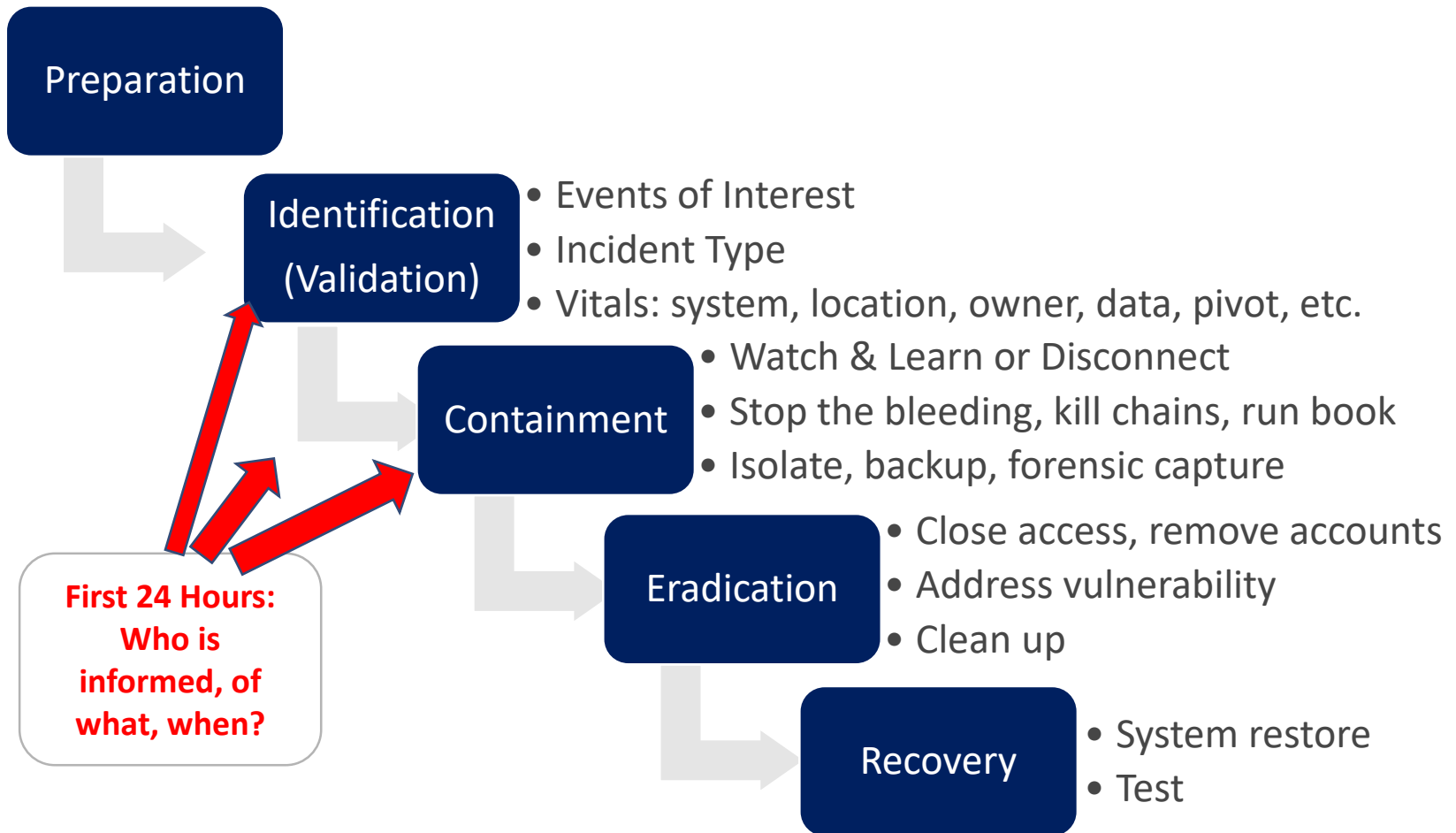
IDENTIFY WHAT HAS BEEN LOST (CONTAIN.)

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

CONTAINMENT (CONT.)

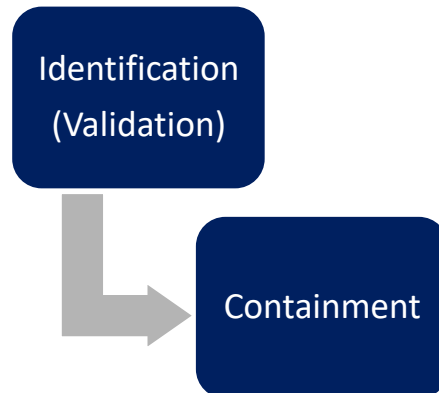
- Know reasonably well before going public:
- Incident is not ongoing
- Type of incident
- Size of breach
- Medium of data: hard copy, electronic or both?
- Location, jurisdictions and controlling law
- Timing of incident:
 - First discovered
 - Internal communications
 - Data affected, elements compromised

INCIDENT HANDLING LIFECYCLE



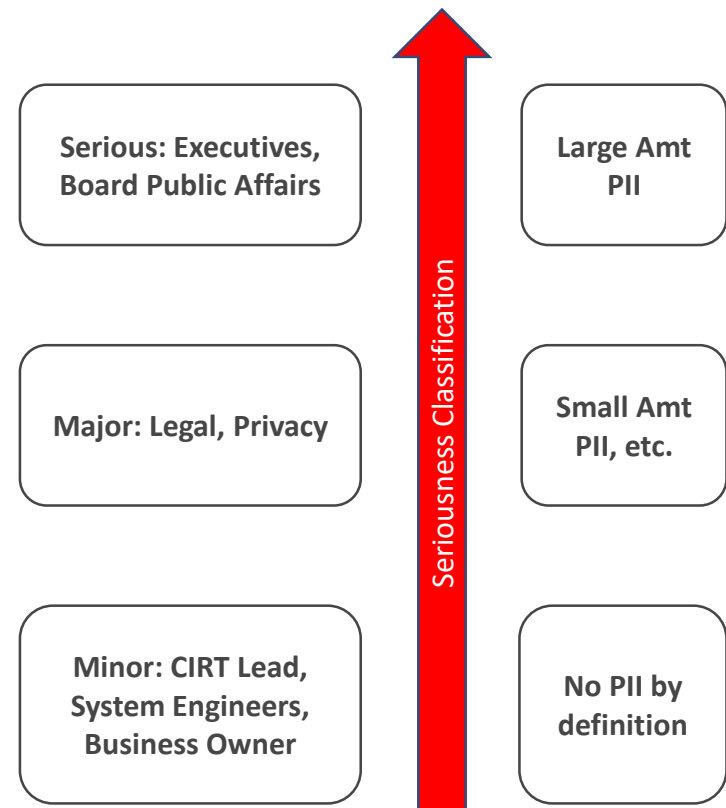
INTERNAL COMMUNICATIONS (IDENTIFICATION)

- Validate suspected incident first!
- Incident classification determines stakeholders (Minor, Serious, Major)
- Don't raise false alarms
- When to notify (by Incident Response Phase):
 - Upon Identification
 - Notify IRT Lead
 - Upon Validation, Notify:
 - Minor: System Owner, Engineers
 - Minor: CISO, Affected Business Line
 - Serious: General Counsel, Compliance, Privacy
 - Major: Executives, Board
 - Major: Insurance Broker
 - Upon Containment:
 - 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

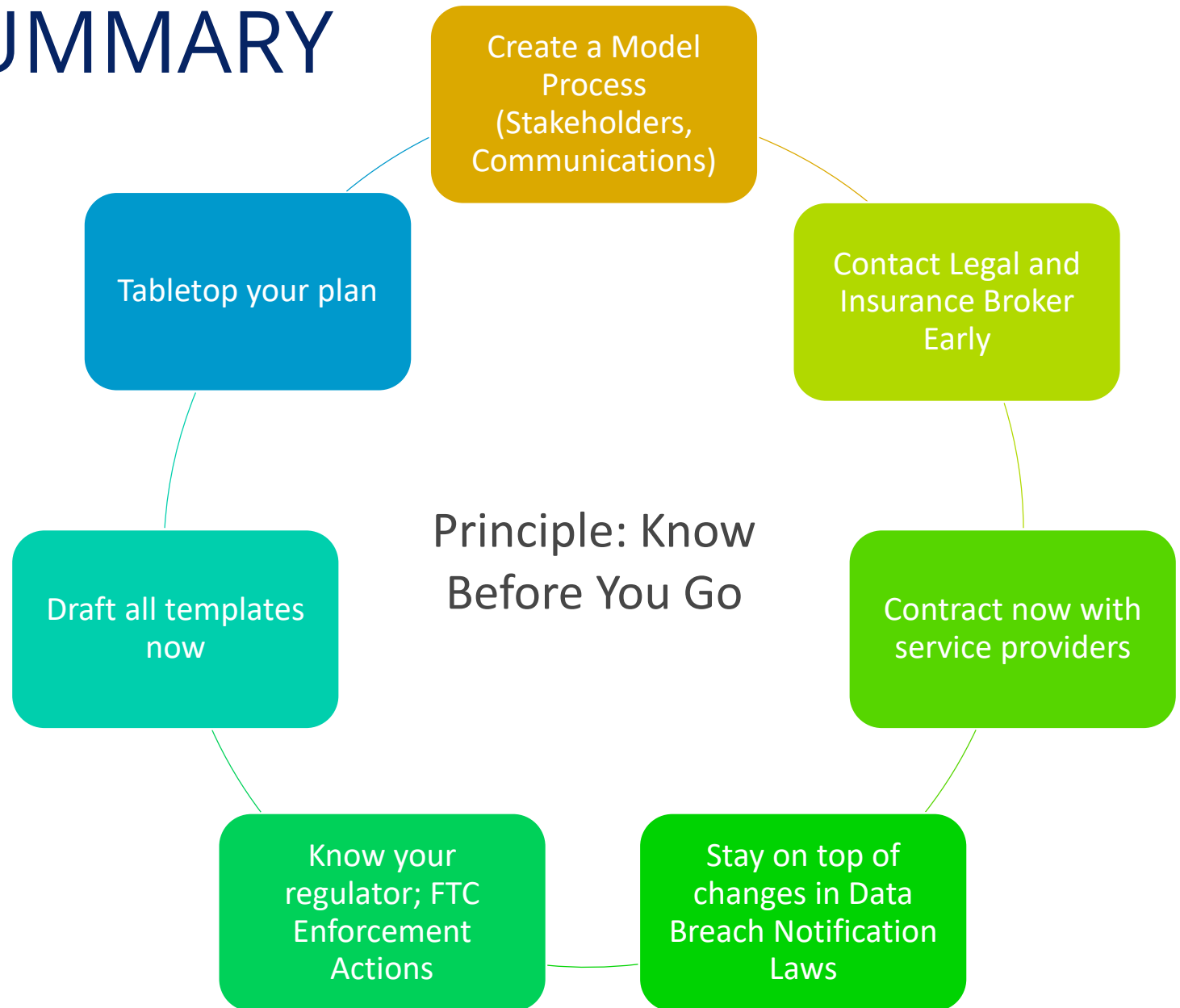
Use working copies for analysis while preserving original drives

Advanced attacks are only discovered in RAM, do not write to drive

Close all outbound data exfiltration channels

Close and patch all vulnerabilities

SUMMARY



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.

THANK YOU!



RICH SPILDE

rdspilde@hollandhart.com

303.473.4808