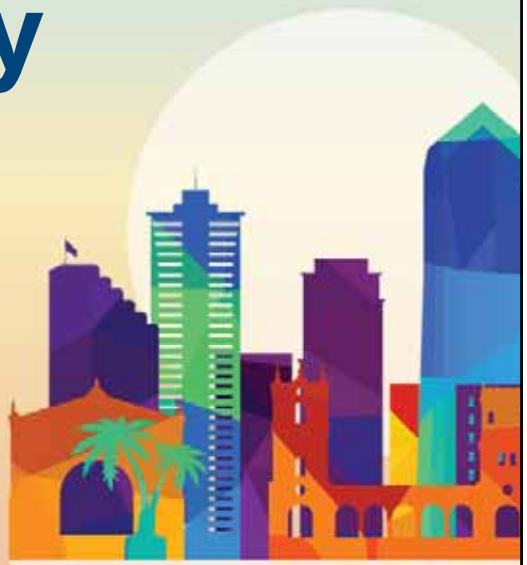
Best Practices in Health Plan Cybersecurity

Jason N. Sheffield, J.D.
National Director of Compliance
The Baldwin Group
Atlanta, Georgia



International Foundation OF EMPLOYEE BENEFIT PLANS

Agenda

- **Part I**
  - Understanding the Application of HIPAA's Security Rule
- **Part II**
  - Defining the Cybercrime Threat
- **Part III**
  - HIPAA as a Defense Against Cyber Attacks
- **Part IV**
  - Detection of Cybercrime and Related Events
- **Part V**
  - Identifying and Responding to a HIPAA Security Breach Event
- **Part VI**
  - Summary of Key Takeaways for Cyber Defense
- **Part VII**
  - Security Rule Implementation Specifications

Learning Objectives

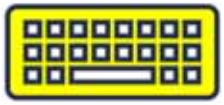
- **This educational program is designed to provide participants with knowledge and understanding related to the following learning objectives:**
  - Define and understand cybercrime as the foremost immediate and decisive threat to the operation and integrity of employee benefit plan administration.
  - Learn to identify types of cybercrime and their variants; in particular, malware deployed for the primary purpose of activating ransomware within a networked environment.
  - Learn and understand core concepts underlying planning, development, implementation, and activation of cybersecurity defensive strategies.
  - Learn and understand the components of responsive breach and post-breach security risk analyses performed upon occurrence of a cybercrime event affecting the organizational technology environment.
  - Understand and apply action steps indicated in the identification, partitioning, termination, and restoration of technology environments impacted by cybercrime events.

Part I:
Understanding the Application of HIPAA's Security Rule

Scope of the HIPAA Security Rule

CREATION

- The Security Rule governs the creation of PHI.
- Creation occurs when:
  - Provider documents a patient visit;
  - Insurer reviews a claim appeal; *and others*.



RECEIPT

- The Security Rule governs the receipt of PHI.
- Receipt occurs when:
  - Insurer receives encounter information from provider;
  - Plan sponsor receives claim audit; *and others*.

MAINTENANCE

- The Security Rule governs maintenance of PHI.
- Maintenance occurs when:
  - Third-party provides storage for backups with PHI;
  - Plan sponsor backs-up data on a drive or other media; *and others*.

TRANSFER

- The Security Rule governs the transfer of PHI.
- Transfer occurs when:
  - Employer sends enrollment to insurer;
  - Insurer sends data for third-party storage; *and others*.

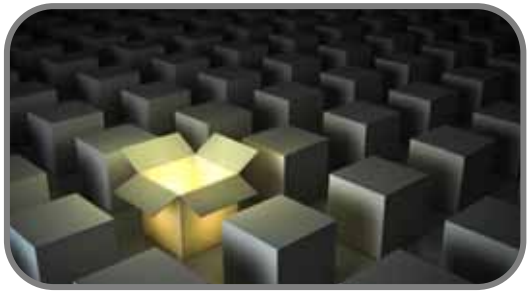
Protection of e-PHI

- **The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI.**
- **Specifically, covered entities must:**
  - Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
  - Identify and protect against reasonably anticipated threats to the security or integrity of the information;
  - Protect against reasonably anticipated, impermissible uses or disclosures; and,
  - Ensure compliance by their workforce.

Defining Compliance

- **The Security Rule's confidentiality requirements support the Privacy Rule's prohibitions against improper uses and disclosures of PHI.**
  - The Security Rule defines "**confidentiality**" to mean that e-PHI is not available or disclosed to unauthorized persons.
- **The rule also promotes the two additional goals of maintaining the integrity and availability of e-PHI.**
  - Under the Security Rule, "**integrity**" means that e-PHI is not altered or destroyed in an unauthorized manner.
  - "**Availability**" means that e-PHI is accessible and usable on demand by an authorized person.

Understanding Specific Terminology



- Vulnerability -

"A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally or intentionally) and result in a security breach."

- Threat -

"The potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability (e.g., natural, human, or environmental threats)."

- Risk -

"A function of (1) the likelihood of a given threat triggering or exploiting a particular vulnerability; and (2) the resulting impact upon the organization or the covered entity."

Part II:
Defining the Cybercrime Threat

Exponential Growth and Costs of Cybercrime

Selected Health Plan Breaches:

2015, Anthem Inc.:

Breach of medical information for 78.8 million people.

2022, Partnership HealthPlan of California:

Theft of 854,913 current and former health plan members' data including diagnoses, treatment and prescription data.

2024, Change Healthcare:

Massive breach affecting the data of one-in-three American citizens.

The healthcare industry faces the highest average data breach cost at over $10.93 million.

IBM Security - Cost of a Data Breach Report 2023.

20% of a healthcare organization's sensitive data is affected by ransomware, but just 6% for others.

https://www.healthcaredive.com/news/healthcare-ransomware-sensitive-data-rubrik-zero-labs/714215/

The 2023 cost of cybercrime was $8 trillion globally and by 2025, it's expected to reach $10.5 trillion.

https://www.usatoday.com/money/blueprint/business/vpn/cybersecurity-statistics/

Health Plan Issues

Suspension of claims payment;

Unable to submit claims; and,

Unable to verify eligibility for benefits.

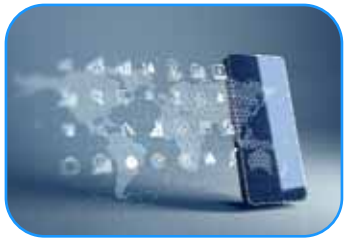
https://www.ama-assn.org/practice-management/sustainability/change-healthcare-cyberattack

Understanding Cybercrime and Its Variations

- **What is cybercrime?**
  - Cybercrime is any **criminal activity** that involves a computer, a networked device or a network.
  - Cybercrimes are committed against computers or devices directly to damage or disable them while computers or networks spread **malware, illegal information, images or other materials.**
  - **Financial enrichment** is often the primary purpose of cybercrime, including different types of criminal activities such as ransomware attacks, email and internet fraud, identity fraud, and others.
  - Cybercriminals may target **individual information** or **corporate data** for theft and resale.
  - COVID-19's "work from home revolution" **encouraged cybercrime** as workers settled into remote work routines, making it increasingly important to protect and backup data.

Understanding Cybercrime and Its Variations

What are the various types of cybercrime?



Email and Internet Fraud

Identity Fraud

Financial Card Payments

Corporate Theft

Cyberextortion

Ransomware Attacks

Crypto-Jacking

Cyberespionage

Contemporary Malware Variants

Common Types of Malware (2021)[1]

Malware Viruses

- Code inserted into a program or application

Worm Malware

- Malware that replicates without human interaction

Trojan Malware

- Hidden in licensed or otherwise legitimate software

Ransomware

- Known attack that comes with a ransom or demand

Bots or Botnets

- Gains access to devices through malicious coding

Adware Malware

- Malware that involves advertising

Spyware

- Collects sensitive information for fraudulent purposes

Rootkits

- Grants remote control of victim's devices

Fileless Malware

- Memory-based malware (rather than file-based)

Malvertising

- Comes hidden on a legitimate internet website

Jackware

- Malware designed to infiltrate machinery/devices via network

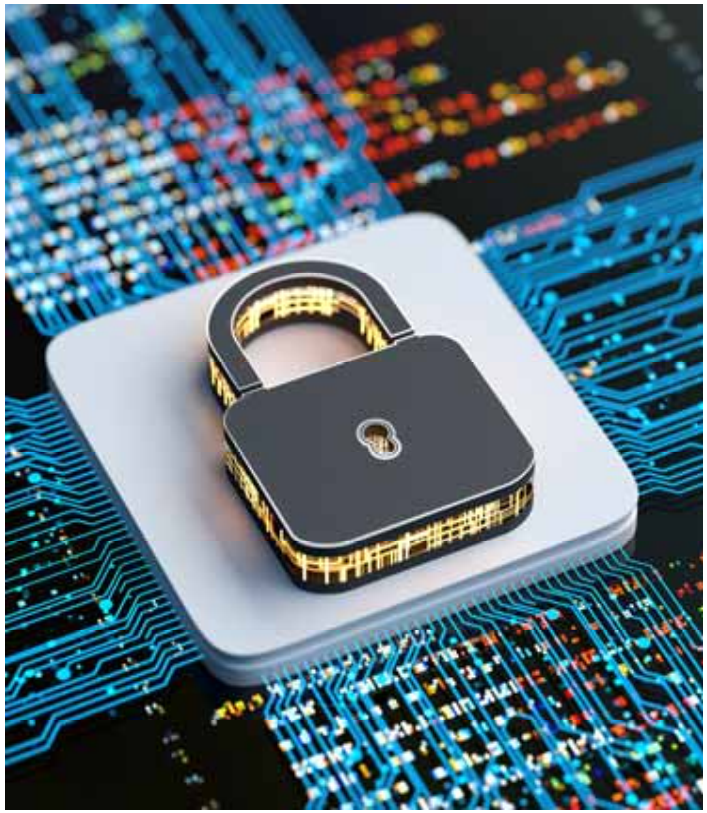
Spam and Phishing

- Social engineering attacks

*See: Norton, US (Aug. 27, 2021): https://us.norton.com/internetsecurity-malware-types-of-malware.html

Understanding the Ransomware Threat

- Ransomware is a type of cyber crime that uses malware (malicious software) **distinct from other variants**
- Its defining characteristic is that it attempts to **deny access to a user's data**, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid.
- After the user's data is encrypted, the ransomware directs the user to **pay the ransom to the hacker** (usually in a cryptocurrency, such as Bitcoin), to receive a decryption key.
- Hackers may deploy ransomware that **destroys or exfiltrates data.**



Part III:
HIPAA as a Defense Against Cyber Attacks

Preemptive Security Design and Implementation

1.
Implement a Security Management Process *including performance of risk assessment*

*CFR §§ 164.308(a)(1), 164.310(c)

2.
Implement procedures to guard against and detect malicious software

*CFR § 164.308(a)(5)

3.
Train users to identify malicious software so they can assist in detecting infections

*CFR § 164.308(a)(5)

4.
Implement access controls to limit access to e-PHI to only those requiring it

*CFR § 164.312(a)(1)

Data and Environmental Security Preparedness

1

BACKUP

- Implement an organizational data backup plan.

2

RECOVERY

- Design, implement, and conduct disaster recovery planning.

3

PLANNING

- Define, implement and test an emergency operation plan.

4

ANALYZE

- Routinely analyze and document the criticality of each application.

5

TESTING

- Assure testing of contingency planning and related operations.

Developing Security Incident Procedures

- Security Rule Incident Procedures
  - Security incident procedures, including procedures for responding to and reporting **security incidents**, are also required by HIPAA.1
  - Security incident procedures should prepare entities to respond to various types of security incidents, including **cybercrime attacks**.
  - Robust security incident procedures should be **designed to**:
    1. Detect and conduct an initial analysis of any cybercrime event;
    2. Contain the impact and propagation of the malware variant(s);
    3. Eradicate any instances of malware and mitigate or remediate any continuing vulnerabilities;
    4. Recover from attacks by restoring data lost during the event and by returning to “business as usual” operations; and,
    5. Define the scope and timing of post-incident activities.

Elements of Security Incident Procedures

DESIGNATE TEAM

- Designate personnel (internal and external resources) to be members of the security incident response team.

RECORD CONTACTS

- Include contact information for all members of the security incident response team.

DETAIL INCIDENTS

- Detail written identification and determination processes for security incidents.

MANAGE EVENTS

- Include detailed instructions explaining how to manage a security incident.

INVENTORY ASSETS

- Incorporate a prioritized inventory of assets (*computer systems and data*) into the written procedures.

Elements of Security Incident Procedures

FORENSIC ANALYSIS

- Provide instructions for conducting a forensic analysis to identify the extent and magnitude of incidents.

NOTIFICATIONS

- Direct the incident response team to make appropriate internal and external event-related notifications.

EVIDENCE PROCESS

- Outline a process for collecting and maintaining evidence related to security incidents.

AUDIT AND TESTING

- Outline processes for periodic audit and testing of security incident response process.

ARCHIVAL RULES

- Archive process, maintaining narratives, documents, analyses, examinations, and other materials.

The HIPAA Security Risk Process

- The Security Rule's Administrative Safeguards require covered entities to "**implement policies and procedures to prevent, detect, contain, and correct security violations**."
- **This requires implementation of reasonable and appropriate security measures to protect against threats or hazards to the security or integrity of e-PHI, including performance of the security risk process, which involves performance of two distinct operational phases of security related tasks:**
  - First, covered entities conduct a **security risk analysis**, also referred to as the initial "**observations phase**" of the process;
  - Next, covered entities perform the **security management process**, also referred to as the secondary "**actions phase**" of the process.

Security Risk Analysis Outcomes

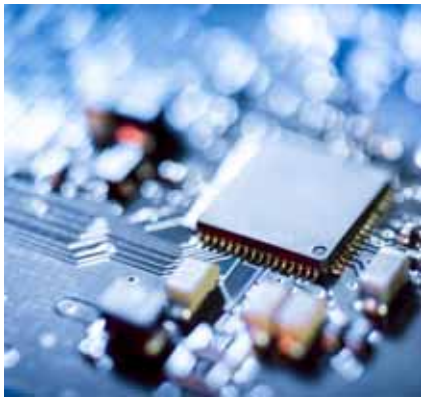
- The outputs derived from a comprehensive Security Risk Analysis ("SRA") operation include:
  - **Satisfaction** of the Covered Entity's SRA requirement;
  - **Charting** of security risks threatening an organization;
  - **Correction** and/or reduction of such risk trajectories;
  - **Development** of Security Incident Procedures; and,
  - **Creation** of a secure environment to support the confidentiality, availability, and integrity of an organization's e-PHI.

Part IV:
Detection of Cybercrime Related Events

Signs of a Cyberattack or Cyber Event

USER REPORT

A user's realization that a link that was clicked on, a file attachment was opened, or a website was visited which may have been malicious in nature.



FILE RESTRICTION

An inability to access certain files as the malware encrypts, deletes, re-names and/or re-locates data.

SYSTEM ACTIVITY

Increase in activity of the central processing unit (CPU) of a computer and/or disk activity for no apparent reason.

NETWORK ACTIVITY

Detection of suspicious network communications between the malware variant and the attackers' control server(s).

Initial Detection of a Cybercrime Event

- **Initial Analysis of the Cyber Attack:**
  1. **Determine the scope of the incident to identify the affected "SAND":**
     - ***S****ystems*, including any components that transform, store, transport, or control materials, energy, etc.;
     - ***A****pplications*, including mobile apps, cloud computing, artificial intelligence, virtual and augmented reality, blockchain, and others;
     - ***N****etworks*, including hardware, software, and communication techniques used to develop and sustain computer networks; and,
     - ***D****evices*, such as shared computers, cellular phones, smartphones, digital cameras, video cameras, audio recording devices, and other electronic devices.
  2. **Determine the origination of the incident;**
  3. **Determine whether the incident is ongoing, or if the agent propagated additional incidents within the environment; and**
  4. **Determine how the incident occurred (e.g., tools and attack methods used, vulnerabilities exploited).**

First Steps for an Affected Organization

INITIATE
RESPONSE PLAN

- The presence of malware is a security incident.
- Initiate the Security Incident Response Plan and activate Security Incident Procedures.

SEGREGATE
AFFECTED SYSTEMS

- Disconnect and isolate infected “SANDs” to halt further propagation in:
  - Systems;
  - Applications;
  - Networks; and,
  - Devices.

NOTIFY
LAW ENFORCEMENT

- Contact the local FBI field office and/or the United States Secret Service field office.
- These agencies coordinate to pursue cybercriminals and to assist victims.

** *See*: Appendix A – Quick Response Checklist from OCR*

Post-Breach Action Steps for an Organization

1. Contain the Damage

- Containment
- Cross-Containment

2. Eradicate All Occurrences

- Eradication
- Mitigation
- Forensics

3. Return to "Status Quo"

- Restoration
- Operations

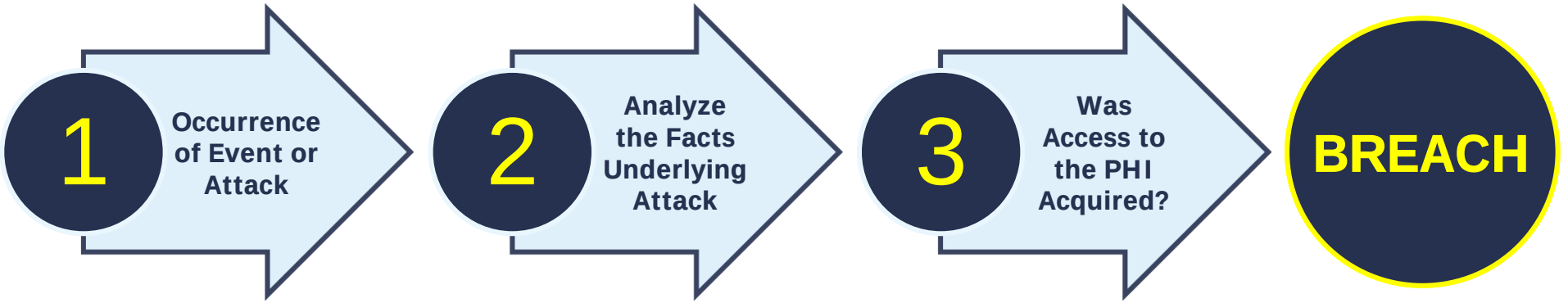
4. Post-Incident Analysis

- Post-Incident Activities
- Related Obligations
- Notice

Part V:
Identifying and Responding to a HIPAA Security Breach Event

Defining a HIPAA Security Breach

A fact-specific analysis is required to determine if an event is a HIPAA security breach:



"...[T]he acquisition, access, use, or disclosure of PHI (*or e-PHI*) in a manner not permitted under the [HIPAA Security Rule] which compromises the security or privacy of the PHI (*or e-PHI*)."

The Presumption of Breach

- **A covered entity must demonstrate that there is a "…low probability that PHI has been compromised," based on the factors set forth in the Breach Notification Rule.**
  - Otherwise, a breach of PHI is **presumed to have occurred.***
  - If a breach has occurred, the entity must comply with the **breach notification requirements** by providing breach notification to:
    1. **Affected individuals** without unreasonable delay;
    2. **The Secretary of HHS** *(considering both small and large breaches)*; and
    3. **Local media outlets** *(for breaches affecting 500 or more individuals)*.

Demonstrating a "Low Probability" of Disclosure

Required Risk Assessment: First Factor

- **Nature and Extent.** The first factor requires an analysis of the nature and the extent of the PHI involved in the breach.
- **Types of Identifiers.** This includes analysis of the types of identifiers disclosed and the likelihood of re-identification of such identifiers by the cybercriminal.

Required Risk Assessment: Second Factor

- **Malicious Actor.** The second factor requires the entity to analyze the event to ascertain the identity of the malicious actor to whom the disclosure was made.
- **Expert Engagement.** The analysis required under the second factor will likely involve the engagement of forensic investigators and/or federal law enforcement.

Required Risk Assessment: Third Factor

- **Unlawful Disclosure.** The third factor requires consideration of whether the PHI was in fact viewed and/or exfiltrated.
- **Assumption of Disclosure.** If the entity is unable to ascertain whether the PHI was viewed, it must assume the attack was successful and that disclosure occurred.*

Note: Encrypted PHI that remains encrypted throughout an attack does create a presumption of unlawful disclosure of PHI.

Required Risk Assessment: Fourth Factor

- **Risk Mitigation.** The fourth factor requires an analysis of the affected entity's risk mitigation activities.
- **Specific Measures.** Detail specific measures taken to reduce resulting harms (*data backups, robust contingency plans with data recovery, test restoration logs, etc.*).

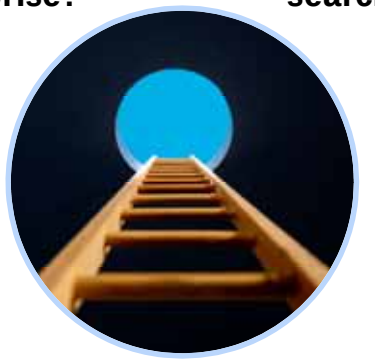
Understanding the Malware Variant

What algorithmic steps does the malware perform?

Can the variant propagate throughout an entity's enterprise?

What types of data is the malware is searching to exploit?

Does the malware attempt to exfiltrate data?



Does the malware deposit hidden software for future access?

Establishing a Low Probability of Compromise

- The risk assessment must be thorough, completed in good faith, and reach conclusions that are reasonable given the circumstances.
- Covered entities and business associates must maintain supporting documentation of the breach assessment, documenting: Assessment conclusions, applicable exceptions and notice operations.

Is an Attack Upon Encrypted Data Noticeable?

Is a Post-Breach Risk Assessment Required?

- If the acquired or viewed PHI was **secured** by a technology or methodology specified by the Secretary, the entity **would not be required to conduct a risk assessment** to determine whether a low probability of compromise existed, and **breach notifications would not be required**.

Effects of Encryption

1. **Electronic PHI has been encrypted if "…An algorithmic process [is used] to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key," and**
2. **Such confidential process or key that might enable decryption has not been breached.**

Breach of Secured PHI Is Not a Security Incident

Data At Rest

- **Data at Rest.** Encryption processes for **data at rest** are consistent with National Institute of Standards and Technology:
- **Separate Storage.** To avoid breach of confidential processes or keys, decryption and encryption tools should be stored on a device or location **separate from the data**.

Data In Motion

- **Data in Motion.** Encryption processes for **data in motion** are those which comply, as appropriate, with NIST Special Publications.

Data Disposal

- **Disposal of Data.** Media on which the PHI is **stored or recorded** has been destroyed in one of the following ways:
  - **Hard Copies.** Paper, film, or other hard copy media have been **shredded or destroyed**.*
  - **Digital Copies.** Electronic media have been **cleared, purged, or destroyed**.

*Note that redaction is specifically excluded as a means of data destruction.

Understanding the Ransomware Threat

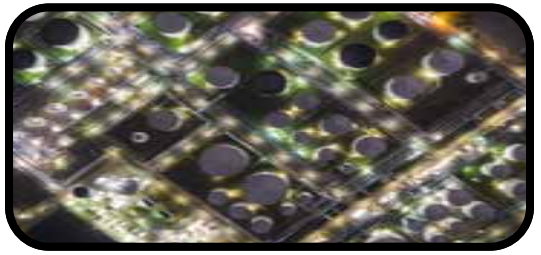
- **Ransomware Payments May Constitute Sanctionable Conduct***
  - Ransomware attacks have increased **substantially** across the last decade.
  - Cybercriminals recognize reliance on distributed networks and have taken advantage of **remote workplace environments** to attack all industries.
  - An Advisory Opinion from Treasury's Office of Foreign Assets Control ("OFAC") points to FBI reports identifying a 21% increase in reported ransom cases and a **225% increase in associated losses** from 2019-2021.
  - Companies facilitating ransomware payments encourage future ransomware and may also **violate OFAC regulations resulting in sanctionable conduct.**

Best Practices May Mitigate Sanctions*

- **OFAC may impose civil penalties for sanctions violations even if the entity or person did not know or have reason to know that it was engaging in a prohibited transaction.**
  - Implement a "risk-based compliance program to **mitigate exposure** to sanctions-related violations."
  - Consider whether a ransom payment involves a **blocked person** or an **embargoed jurisdiction**.
  - OFAC will consider a company's efforts to **improve cybersecurity practices** when determining whether a company committed a sanctionable violation.

Best Practices May Mitigate Sanctions*

1) Maintain offline (physical and/or cloud-based) backups of PHI and other data



2) Develop and routinely test robust security incident plans and related procedures

3) Install and enforce authentication protocols for all authorized users

Part VI:
Summary of Key Takeaways for Cyber Defense

Cybersecurity Best Practices Checklist

Establish a security culture

Monitor mobile device use

Reward good computer habits

Use and maintain a firewall

Install anti-virus defenses

Control physical access

Control network access

Enforce password policies

Utilize dual-factor technology

Keep on planning and adapting

Your Feedback Is Important.
Please Scan This QR Code.

Session Evaluation