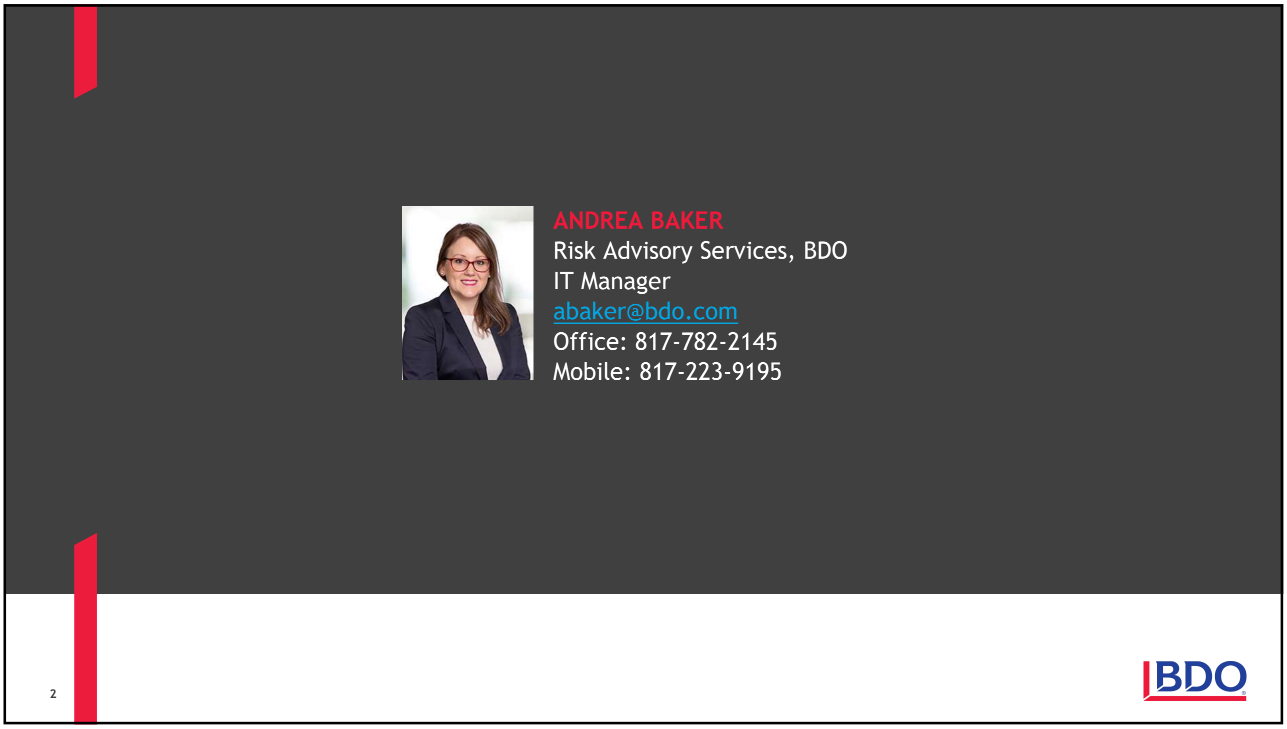
CYBERSECURITY AND SAFEGUARDING HEALTHCARE RECORDS

BDO

1



ANDREA BAKER
Risk Advisory Services, BDO
IT Manager
abaker@bdo.com
Office: 817-782-2145
Mobile: 817-223-9195

2

BDO

2

Topics

This discussion contains the following topics:

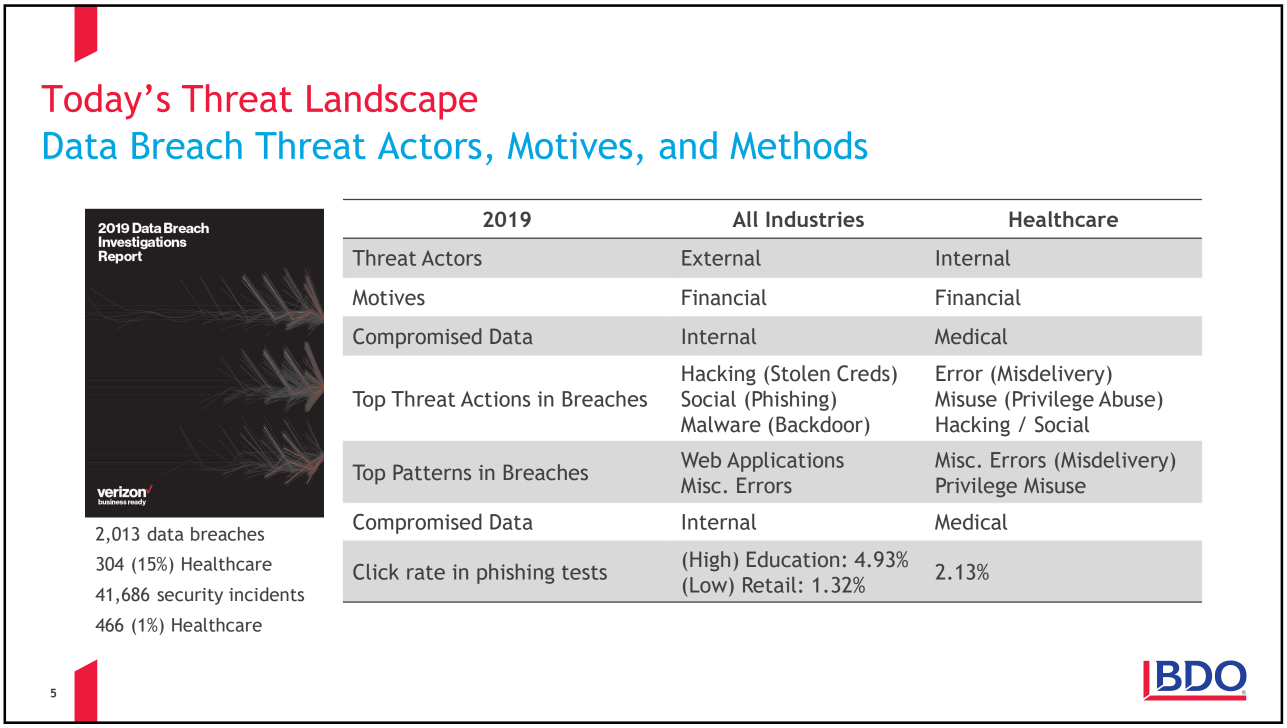
- Topic 1: Today’s Threat Landscape
- Topic 2: IT Security Maturity Assessment
- Topic 3: Cybersecurity and Its Impacts on Healthcare

Question

The majority of breaches are associated with what kind of threat actors?

A. Internal

B. External



Today’s Threat Landscape
Data Breach Threat Actors, Motives, and Methods

2019 Data Breach Investigations Report
verizon
business ready

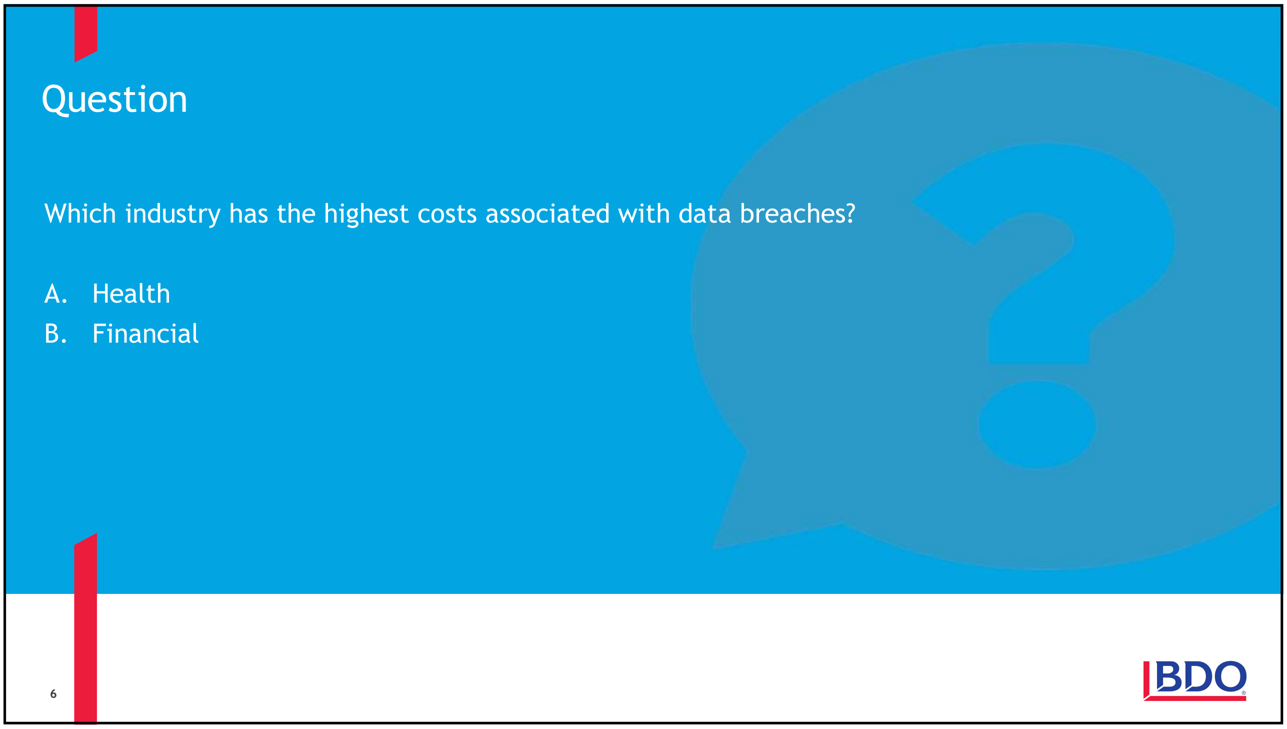
2,013 data breaches

304 (15%) Healthcare

41,686 security incidents

466 (1%) Healthcare

2019	All Industries	Healthcare
Threat Actors	External	Internal
Motives	Financial	Financial
Compromised Data	Internal	Medical
Top Threat Actions in Breaches	Hacking (Stolen Creds) Social (Phishing) Malware (Backdoor)	Error (Misdelivery) Misuse (Privilege Abuse) Hacking / Social
Top Patterns in Breaches	Web Applications Misc. Errors	Misc. Errors (Misdelivery) Privilege Misuse
Compromised Data	Internal	Medical
Click rate in phishing tests	(High) Education: 4.93% (Low) Retail: 1.32%	2.13%

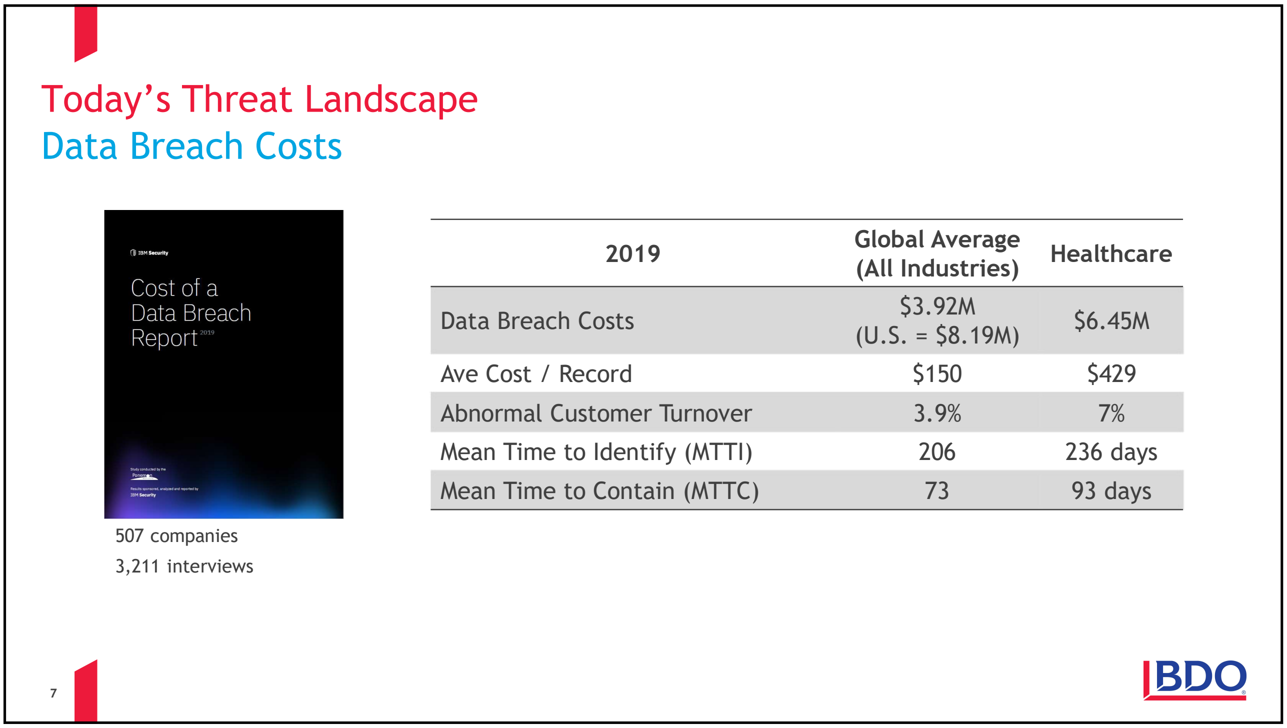


Question

Which industry has the highest costs associated with data breaches?

A. Health

B. Financial



Today’s Threat Landscape
Data Breach Costs

IBM Security

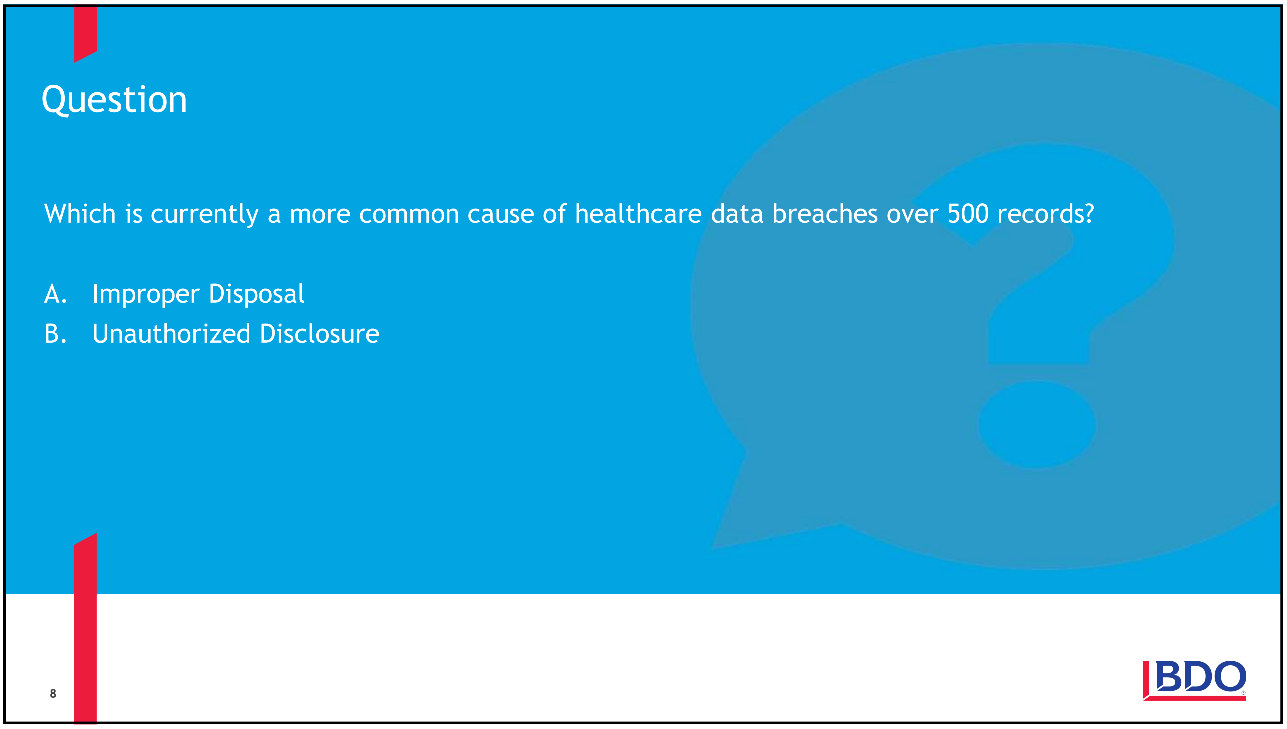
Cost of a Data Breach Report 2019

507 companies

3,211 interviews

2019	Global Average (All Industries)	Healthcare
Data Breach Costs	$3.92M (U.S. = $8.19M)	$6.45M
Ave Cost / Record	$150	$429
Abnormal Customer Turnover	3.9%	7%
Mean Time to Identify (MTTI)	206	236 days
Mean Time to Contain (MTTC)	73	93 days

BDO



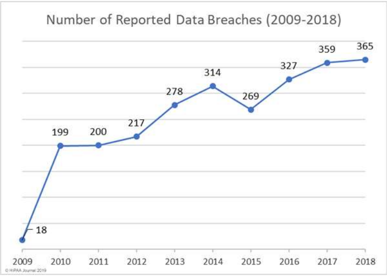
Question

Which is currently a more common cause of healthcare data breaches over 500 records?

A. Improper Disposal
B. Unauthorized Disclosure

BDO

Today’s Threat Landscape
Healthcare Data Breaches per Year



- 2018:
  - Hacking/IT Incidents (158 breaches)
  - Unauthorized Access/Disclosures (143 breaches)
  - Loss/Theft (55 breaches)
  - Improper Disposal (9 breaches)
- Data breaches reported at a rate of more than 1 / day
- Greatest number of records breached in 2015 (~113 M records)
- Fewest records breached in 2012 (~2.8 M records)
- 2018 – record breaking year for HIPAA fines and settlements
  - $28.6 M from covered entities and business associates

Question

Which covered entity had the largest healthcare data breach since 2009?

A. Premera Blue Cross

B. Anthem Inc.

Today’s Threat Landscape
Case Studies

Anthem

- 2015
- 78.8M individuals
- Hacking/IT Incident

SAIC

- 2011
- 4.9M individuals
- Loss

ERS

- 2018
- 1.2M individuals
- Unauthorized Access/Disclosure

AvMed

- 2010
- 1.7M individuals
- Theft

AccuDoc Solutions

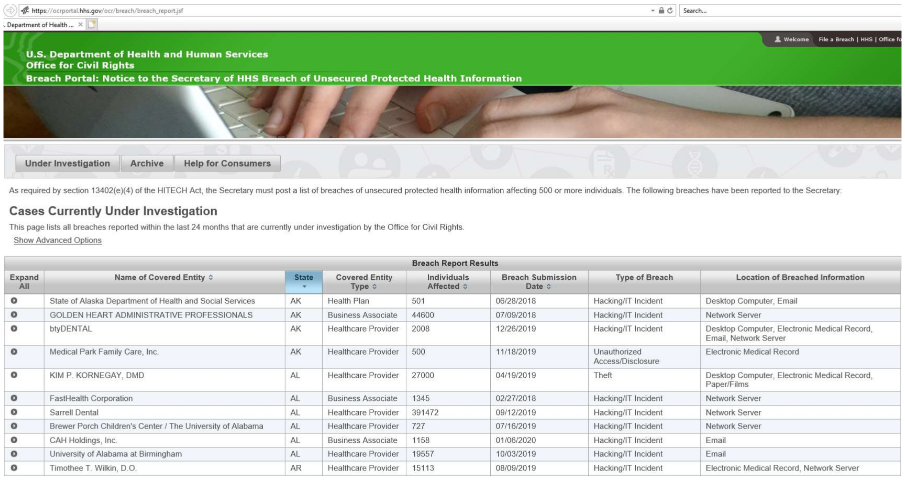
- 2018
- 2.6M individuals
- Hacking/IT Incident

UnityPoint Health

- 2018
- 1.4M individuals
- Hacking/IT Incident

BDO

Today’s Threat Landscape
Office for Civil Rights (OCR) Breach Portal


https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
Search...
. Department of Health ...
Welcome
File a Breach | HHS | Office fo

U.S. Department of Health and Human Services
Office for Civil Rights
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

Under Investigation
Archive
Help for Consumers

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. The following breaches have been reported to the Secretary:

Cases Currently Under Investigation

This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

Show Advanced Options

Breach Report Results

Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
●	State of Alaska Department of Health and Social Services	AK	Health Plan	501	06/28/2018	Hacking/IT Incident	Desktop Computer, Email
●	GOLDEN HEART ADMINISTRATIVE PROFESSIONALS	AK	Business Associate	44600	07/09/2018	Hacking/IT Incident	Network Server
●	btyDENTAL	AK	Healthcare Provider	2008	12/26/2019	Hacking/IT Incident	Desktop Computer, Electronic Medical Record, Email, Network Server
●	Medical Park Family Care, Inc.	AK	Healthcare Provider	500	11/18/2019	Unauthorized Access/Disclosure	Electronic Medical Record
●	KIM P. KORNEGAY, DMD	AL	Healthcare Provider	27000	04/19/2019	Theft	Desktop Computer, Electronic Medical Record, Paper/Films
●	FastHealth Corporation	AL	Business Associate	1345	02/27/2018	Hacking/IT Incident	Network Server
●	Sarrell Dental	AL	Healthcare Provider	391472	09/12/2019	Hacking/IT Incident	Network Server
●	Brewer Porch Children's Center / The University of Alabama	AL	Healthcare Provider	727	07/16/2019	Hacking/IT Incident	Network Server
●	CAH Holdings, Inc.	AL	Business Associate	1158	01/06/2020	Hacking/IT Incident	Email
●	University of Alabama at Birmingham	AL	Healthcare Provider	19557	10/03/2019	Hacking/IT Incident	Email
●	Timothee T. Wilkin, D.O.	AR	Healthcare Provider	15113	08/09/2019	Hacking/IT Incident	Electronic Medical Record, Network Server

BDO

IT Security Maturity Assessment
Cybersecurity Audit

Overview

An IT security maturity assessment is used to give a company a high level idea of their current IT state by assessing the risk and maturity levels of their IT environment. This is done by determining any gaps in program design, policies, standards, and procedures.

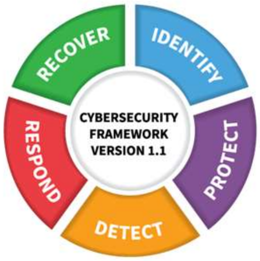
Framework

Our approach and methodology leverages the National Institute of Standards & Technology (NIST) Cybersecurity Framework to evaluate the cybersecurity maturity and level of risk, in comparison to other organizations of similar size and industry.

IT Security Maturity Assessment
NIST Cybersecurity Framework

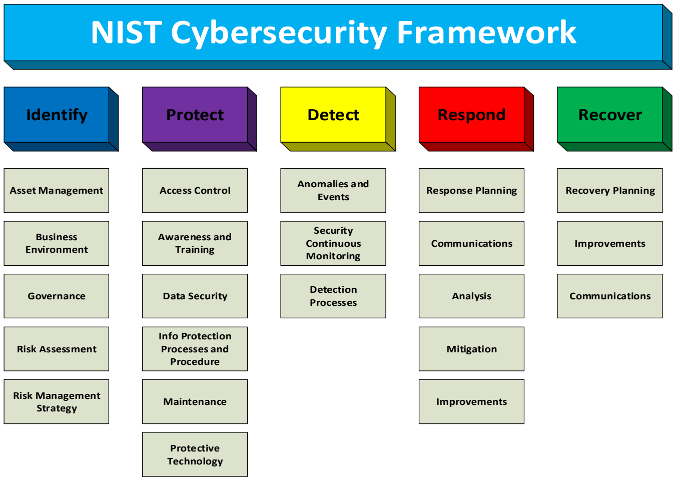
Why NIST?

The NIST Cybersecurity Framework provides a policy framework of computer security guidance for how private sector organizations in the United States can assess and improve their ability to prevent, detect, and respond to cyber attacks.



IT Security Maturity Assessment

NIST Recommended Cybersecurity Components



NIST Cybersecurity Framework

Identify
- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

Protect
- Access Control
- Awareness and Training
- Data Security
- Info Protection Processes and Procedure
- Maintenance
- Protective Technology

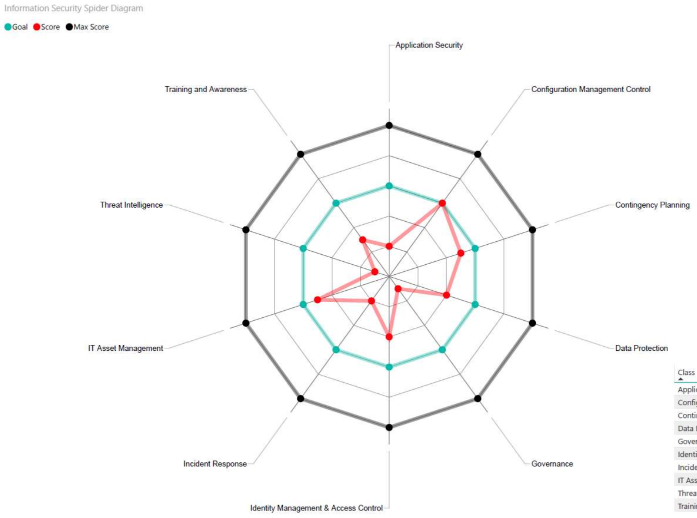
Detect
- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

Respond
- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

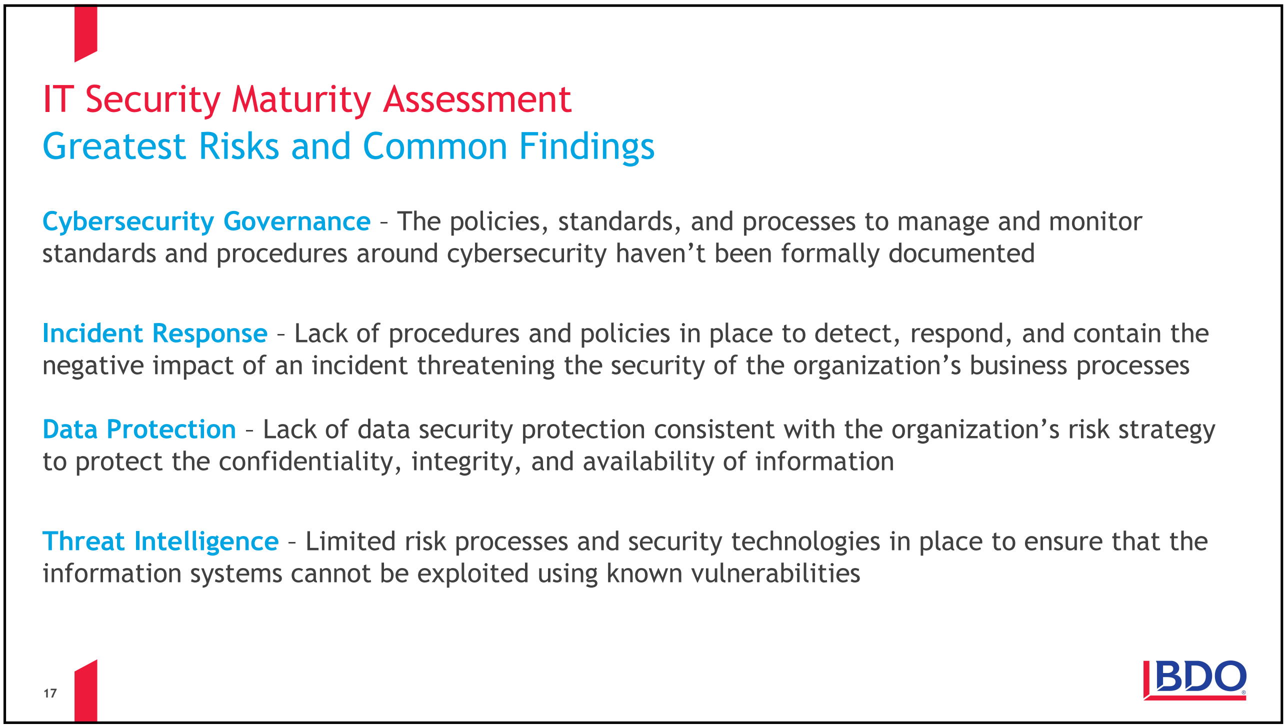
Recover
- Recovery Planning
- Improvements
- Communications

IT Security Maturity Assessment

Risk Scorecard



Class	Score	Goal
Application Security	1.00	3
Configuration Management Control	3.00	3
Contingency Planning	2.50	3
Data Protection	2.00	3
Governance	0.50	3
Identity Management & Access Control	2.00	3
Incident Response	1.00	3
IT Asset Management	2.50	3
Threat Intelligence	0.50	3
Training and Awareness	1.50	3



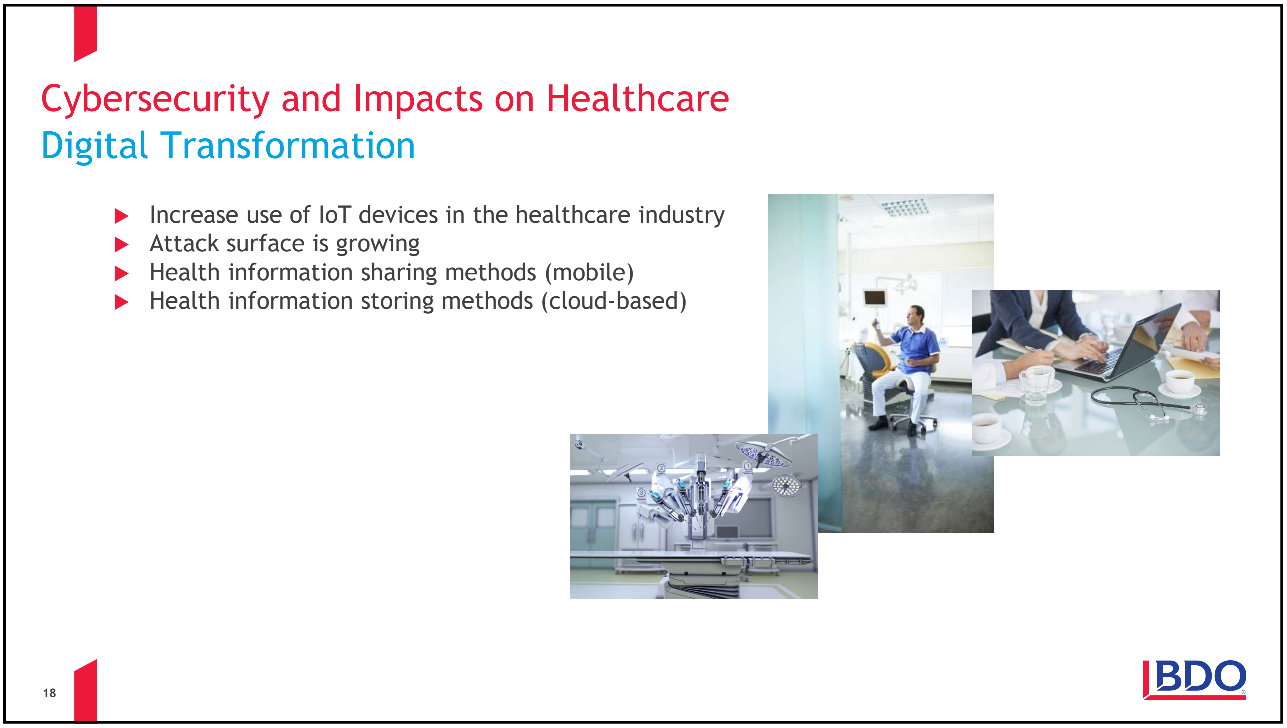
IT Security Maturity Assessment
Greatest Risks and Common Findings

Cybersecurity Governance – The policies, standards, and processes to manage and monitor standards and procedures around cybersecurity haven't been formally documented

Incident Response – Lack of procedures and policies in place to detect, respond, and contain the negative impact of an incident threatening the security of the organization's business processes

Data Protection – Lack of data security protection consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information

Threat Intelligence – Limited risk processes and security technologies in place to ensure that the information systems cannot be exploited using known vulnerabilities



Cybersecurity and Impacts on Healthcare
Digital Transformation

- Increase use of IoT devices in the healthcare industry
- Attack surface is growing
- Health information sharing methods (mobile)
- Health information storing methods (cloud-based)

Cybersecurity and Impacts on Healthcare
Changes in the way we access, transmit, and store health information

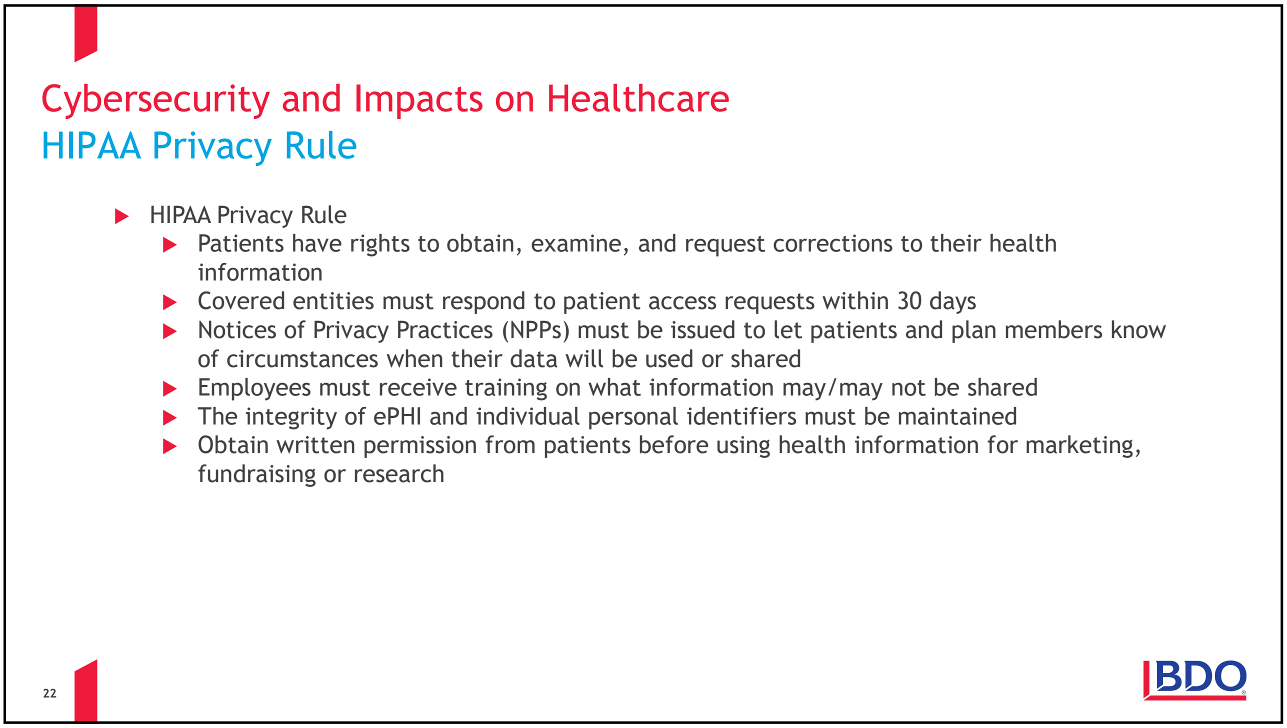
- Websites
- Mobile Access
- Text (SMS)
- Virtual Patient Visits
- Social Media
- Cloud Computing

Cybersecurity and Impacts on Healthcare
Legislation

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - Applies to:
    - <u>Covered Entities</u> - transmit protected health information for transactions for which the Department of HHS has adopted standards
    - <u>Business Associates</u> - provide services to a HIPAA-covered entity which requires them to have access to, store, use, or transmit protected health information
  - Rules include:
    - Security Rule (Safeguards)
    - Privacy Rule
    - Breach Notification Rule
    - Omnibus Rule
    - Enforcement Rule
- The Health Information Technology for Economic and Clinical Health (HITECH) Act – 2009
- The Medicare Access & CHIP Reauthorization Act of 2015 (MARCA)

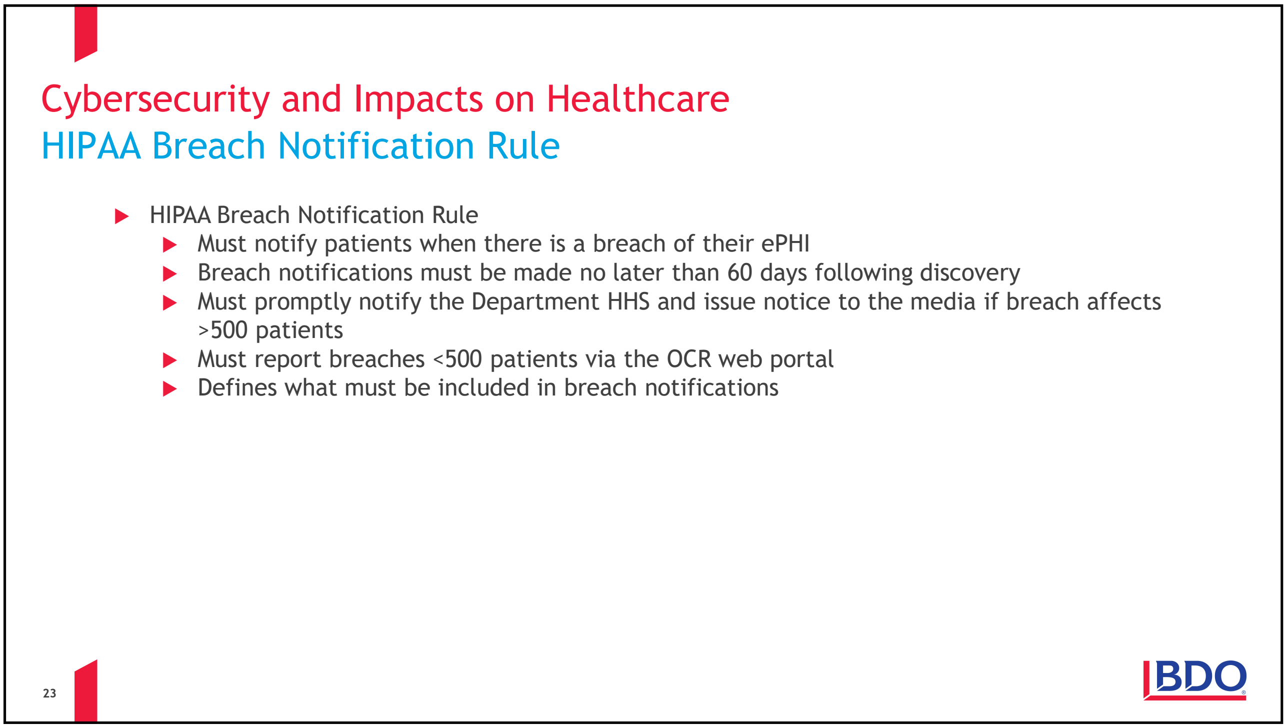
Cybersecurity and Impacts on Healthcare
HIPAA Security Rule

- HIPAA Security Rule
  - Standards that must be applied to safeguard ePHI when it is at rest and in transit
  - Includes “required” and “addressable” safeguards on the HIPAA compliance checklist
  - Three parts:
    - Technology Safeguards
    - Physical Safeguards
    - Administrative Safeguards



Cybersecurity and Impacts on Healthcare
HIPAA Privacy Rule

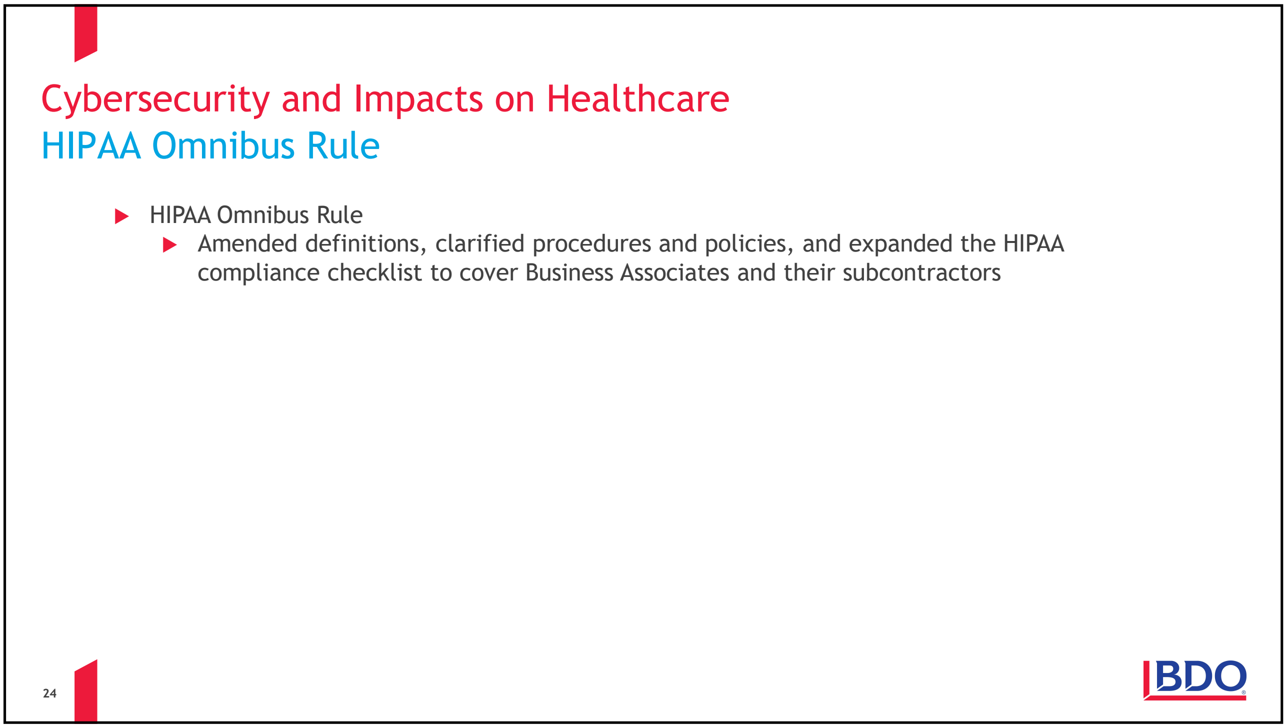
- HIPAA Privacy Rule
  - Patients have rights to obtain, examine, and request corrections to their health information
  - Covered entities must respond to patient access requests within 30 days
  - Notices of Privacy Practices (NPPs) must be issued to let patients and plan members know of circumstances when their data will be used or shared
  - Employees must receive training on what information may/may not be shared
  - The integrity of ePHI and individual personal identifiers must be maintained
  - Obtain written permission from patients before using health information for marketing, fundraising or research



Cybersecurity and Impacts on Healthcare

HIPAA Breach Notification Rule

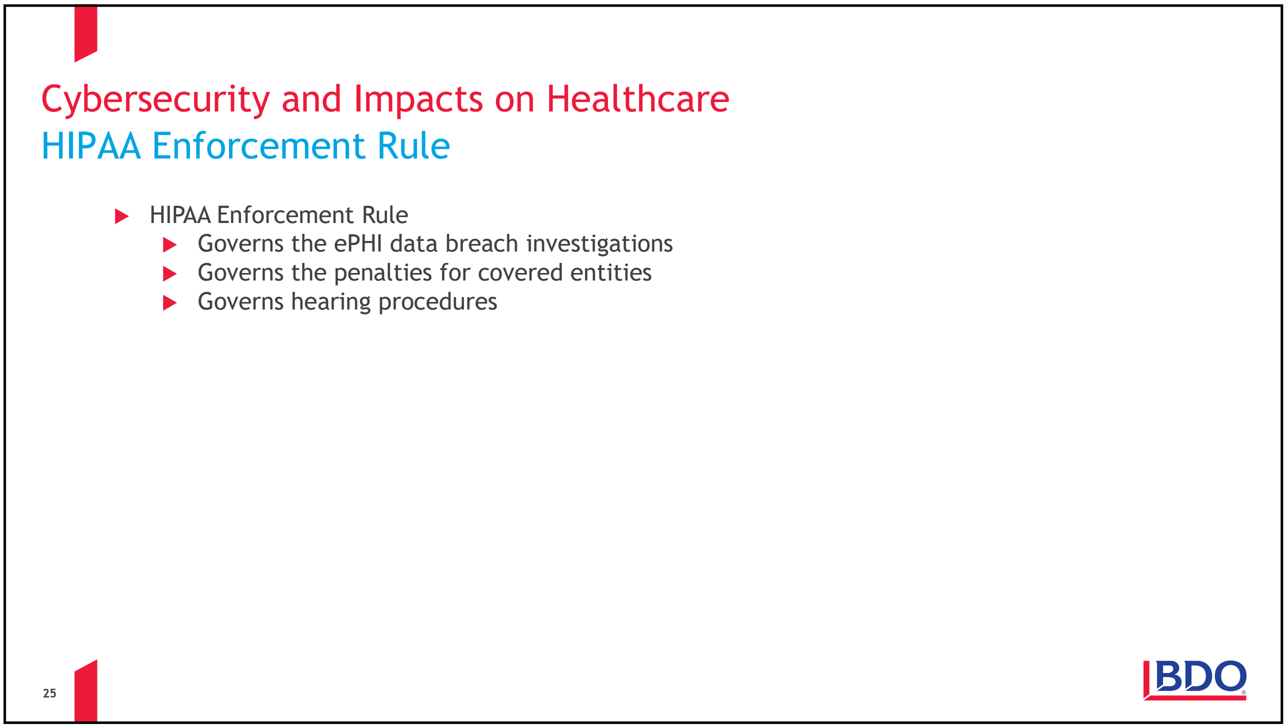
- HIPAA Breach Notification Rule
  - Must notify patients when there is a breach of their ePHI
  - Breach notifications must be made no later than 60 days following discovery
  - Must promptly notify the Department HHS and issue notice to the media if breach affects >500 patients
  - Must report breaches <500 patients via the OCR web portal
  - Defines what must be included in breach notifications



Cybersecurity and Impacts on Healthcare

HIPAA Omnibus Rule

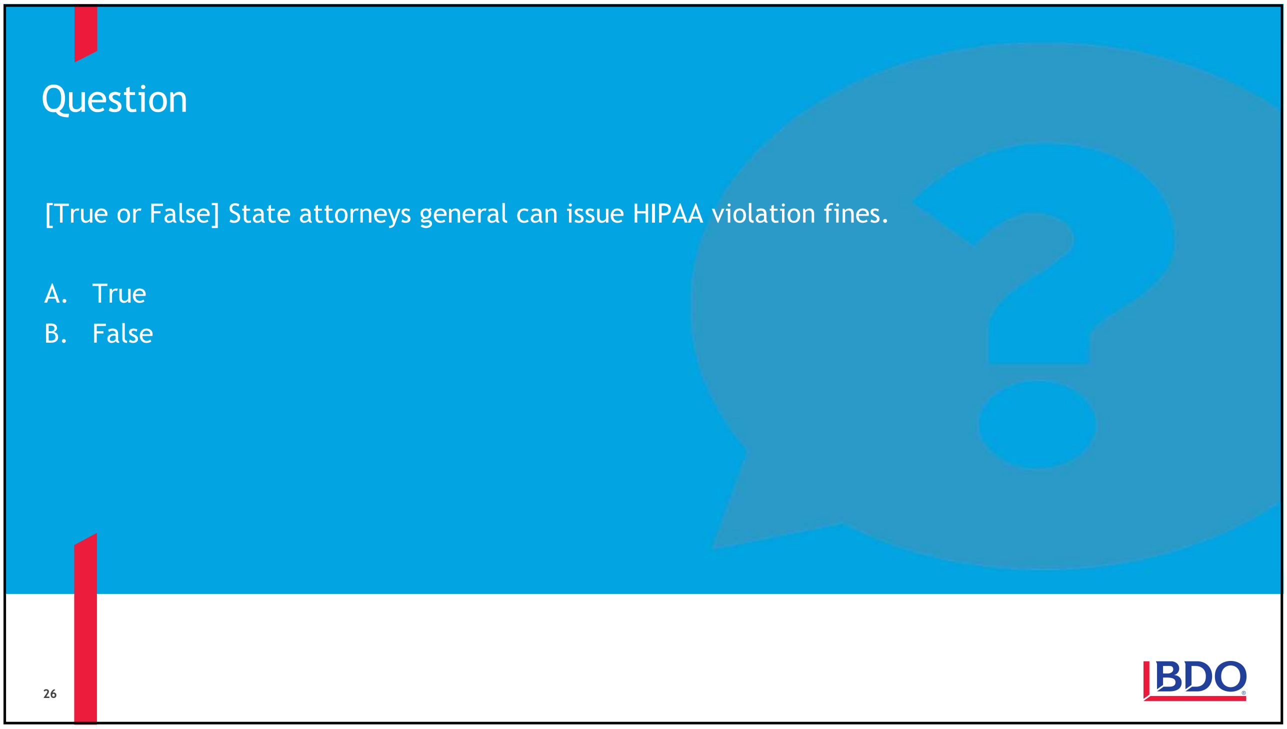
- HIPAA Omnibus Rule
  - Amended definitions, clarified procedures and policies, and expanded the HIPAA compliance checklist to cover Business Associates and their subcontractors



Cybersecurity and Impacts on Healthcare
HIPAA Enforcement Rule

- HIPAA Enforcement Rule
  - Governs the ePHI data breach investigations
  - Governs the penalties for covered entities
  - Governs hearing procedures

25



Question

[True or False] State attorneys general can issue HIPAA violation fines.

A. True
B. False

26

Cybersecurity and Impacts on Healthcare

Legislation

- HIPAA fines issues by:
  - Dept of HHS' Office for Civil Rights (OCR)
  - State Attorneys General
- Violations are usually discovered by:
  - Data breach investigations
  - Compliant investigations
  - Compliance audits

U.S. Department of Health and Human Services
Office for Civil Rights
Complaint Portal Assistant

Question

[True or False] Heart rate and blood pressure information collected from a device manufacturer and/or application that has not been contracted by a HIPAA-covered entity is still considered PHI.

A. True

B. False

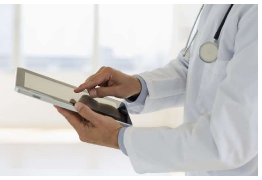
Cybersecurity and Impacts on Healthcare
What is considered Protected Healthcare Information (PHI)

- Any identifiable health information that is used, maintained, stored, or transmitted by a HIPAA-covered entity
  - Names
  - Dates, except year
  - Telephone numbers
  - Geographic data
  - Fax numbers
  - SSN
  - Email addresses
  - Medical record numbers
  - Account numbers
  - Healthcare plan beneficiary numbers
  - Certificate/license numbers
  - Vehicle identifiers (including license plates)
  - Driver's license numbers
  - Web URLs
  - Device identifiers/serial numbers
  - IP addresses
  - Full face photos
  - Biometric identifiers
  - Unique identifiers (numbers/codes)

BDO

Cybersecurity and Impacts on Healthcare
Most Common HIPAA Violations

- Failure to perform risk analysis to identify risks to CIA of PHI
- Failure to enter into a HIPAA-compliant business associate agreement
- Impermissible disclosures of PHI
- Not meeting the breach notification deadline
- Failure to safeguard PHI
- Snooping on health records
- Lack of risk management processes
- Failure to use encryption on portable devices
- Improper disposal of PHI
- Denying or exceeding timeframe to provide access to health records



BDO

Cybersecurity and Impacts on Healthcare
Common Violations by Healthcare Employees

- Emailing ePHI to personal email
- Unattended paperwork / portable devices
- Releasing PHI to unauthorized individual
- Releasing PHI without authorization
- Releasing PHI to third party after authorization expiration
- Failure to perform risk analysis to identify risks to CIA of PHI
- Impermissible disclosures of PHI
- Downloading PHI to unauthorized devices
- Unauthorized access to PHI
- Failure to enter into a HIPAA-compliant business associate agreement

BDO

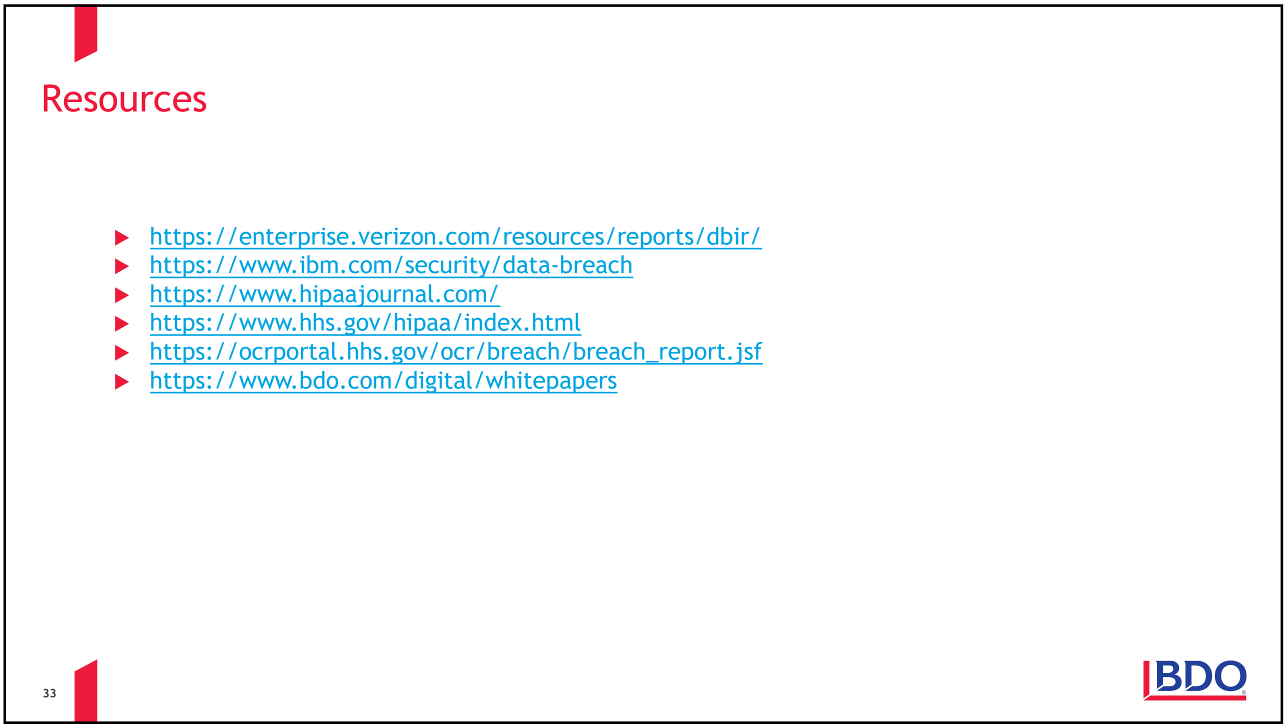
31

Cybersecurity and Impacts on Healthcare
Best Practices

- Data encryption
- Phishing awareness
- Audit logs
- Proper network, software, and cloud-based solution configuration

BDO

32



Resources

- https://enterprise.verizon.com/resources/reports/dbir/
- https://www.ibm.com/security/data-breach
- https://www.hipaajournal.com/
- https://www.hhs.gov/hipaa/index.html
- https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
- https://www.bdo.com/digital/whitepapers

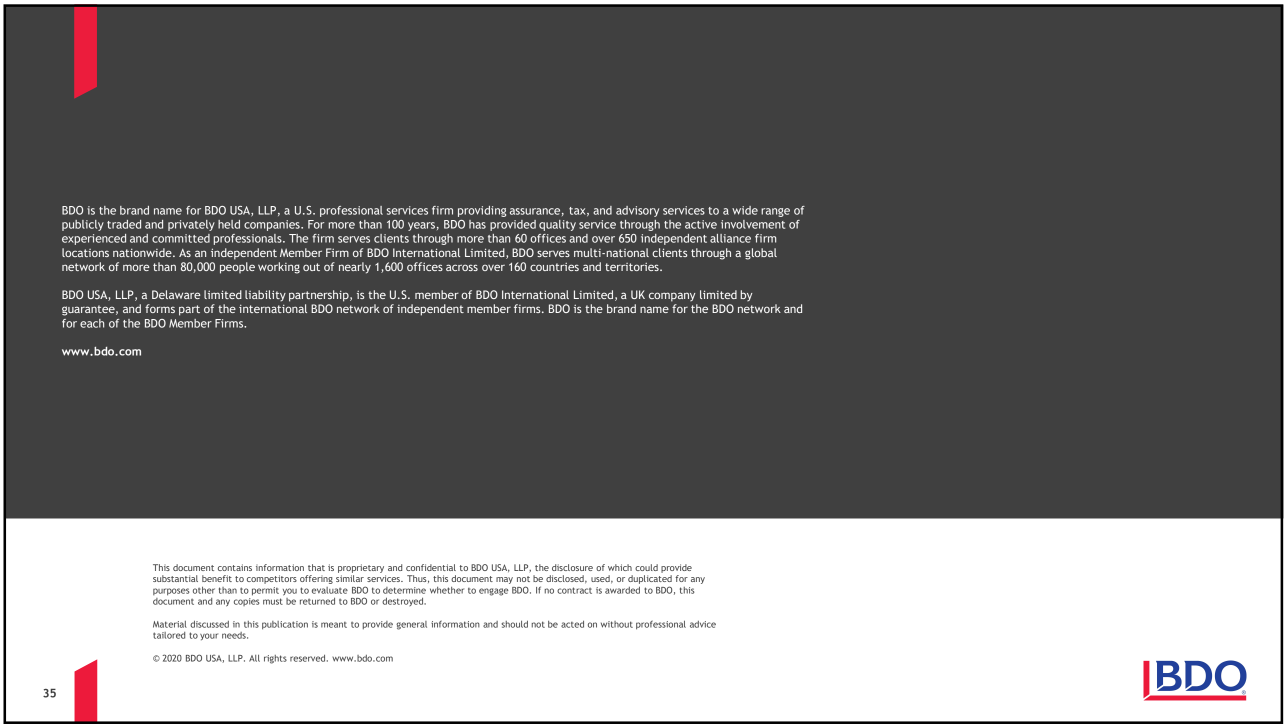
BDO

33

QUESTIONS?

BDO

34



BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 650 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of more than 80,000 people working out of nearly 1,600 offices across over 160 countries and territories.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms.

www.bdo.com

This document contains information that is proprietary and confidential to BDO USA, LLP, the disclosure of which could provide substantial benefit to competitors offering similar services. Thus, this document may not be disclosed, used, or duplicated for any purposes other than to permit you to evaluate BDO to determine whether to engage BDO. If no contract is awarded to BDO, this document and any copies must be returned to BDO or destroyed.

Material discussed in this publication is meant to provide general information and should not be acted on without professional advice tailored to your needs.