



Cyber Defense in Healthcare:

Are You Prepared for the Next Wave of Attacks?

MAY 21, 2024

BDO USA, P.A., a Delaware professional service corporation, 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.



CPE and Support

TECHNICAL SUPPORT

BDO Employees:

888-236-9111

Alliance, International, and Invited Guests:

844-580-6963



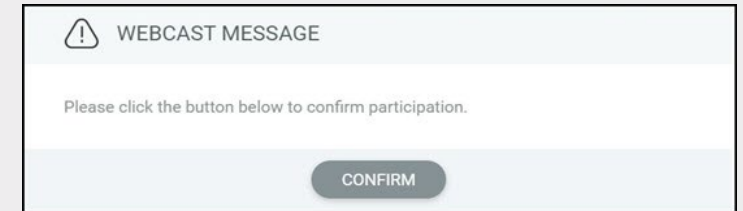
CLOSED CAPTIONS:

Can be found in the bottom right corner of the Media Panel in the center of your screen

CPE PARTICIPATION REQUIREMENTS

To receive CPE credit for this webcast, you must actively participate throughout the program. For each CPE credit hour, you must:

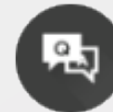
- ▶ Respond to at least 3 checkpoint pop-ups / polls
- ▶ Be in attendance for at least 50 minutes



**SAMPLE CHECKPOINT POP-UP
(POLLS WILL APPEAR IN THE SLIDE PANEL, IF APPLICABLE)**



CHAT: Use the chat to submit public questions and comments during the webinar



Q&A: Submit technical support questions directly to the host by clicking the Q&A icon



HANDOUTS: Click the Handouts icon for helpful resources



TECHNICAL SUPPORT: Click the icon to open the Technical Support Panel

With You Today



COURTNEY BOYNTON

Healthcare Solutions Director

clboynton@bdo.com

Learning Objectives



Identify common cybersecurity threats and risks specific to healthcare organizations



Review where potential weaknesses in your cybersecurity infrastructure might exist



Examine the regulatory environment surrounding healthcare cybersecurity, with a focus on HIPAA compliance



Describe effective strategies to protect your healthcare organization from cyber threats

Today's Panelists



ELIE GERGES

Risk Advisory Services
Senior Manager

egerges@bdo.com



RAJDEEP MUKHERJEE

Management Consulting
Director

rmukherjee@bdo.com



VENSON WALLIN

Healthcare Regulatory &
Compliance Services
Managing Director

vawallin@bdo.com

Our Agenda Today



Current Cybersecurity Landscape in Healthcare




Cybersecurity Threats, Risk & their Impacts for Healthcare Organizations



Building a Secure Healthcare Organization



Regulatory Update



The HHS Office of Civil Rights reported a staggering **264%** increase in healthcare ransomware attacks over the past five years.

Current Cybersecurity Landscape in Healthcare



The **average cost of a healthcare data breach** has now reached an unprecedented **\$11M**, marking a **53% increase since 2020**



A concerning **88% of healthcare organizations reported experiencing a cyberattack in the past year**



Nearly half of the 40 million healthcare records exposed in 2023 were due to attacks targeting healthcare providers' **third-party business associates**



Many **HIPAA violations**, which have led to financial penalties averaging \$346,667 in 2023, **stem from negligence and a failure to conduct comprehensive organization-wide risk assessments**

DISCUSSION QUESTION #1

Do you feel your Information Security Program is adequate for the size and complexity of your organization?

- 1 Yes
- 2 No
- 3 Not sure
- 4 Not applicable

DISCUSSION QUESTION #1

Do you feel your Information Security Program is adequate for the size and complexity of your organization?

POLL RESULTS

1

Yes

2

No

4

Not applicable

Cybersecurity Threats, Risk & their Impacts to Healthcare Organizations



Cyber threats faced by healthcare organizations

- ▶ Social Engineering
- ▶ Ransomware
- ▶ Loss or Theft of Equipment or Data
- ▶ Insider, Accidental or Malicious Data loss
- ▶ Attack against Network connected medical devices
- ▶ Cyberattacks on third parties providing critical services or software solutions



Cybersecurity risks in healthcare

- ▶ Patient Safety
- ▶ Data Privacy and Compliance Risk
- ▶ Third party risk
- ▶ Operational risk
- ▶ Financial Risk
- ▶ Reputational risk



Organizational impact

- ▶ Loss of patient trust/reputational impact
- ▶ Financial loss
- ▶ Legal and regulatory loss
- ▶ Operational/patient care impact (e.g. delays in procedures, longer length of stay, increase in complications and increased mortality rate)

Source of Threats: <https://405d.hhs.gov/cornerstone/hicp#best-practices>

DISCUSSION QUESTION #2

In the past 12 months,
has your organization
performed a HIPAA Risk
Assessment?

1

Yes

2

No

3

Not sure

4

Not applicable

DISCUSSION QUESTION #2

In the past 12 months,
has your organization
performed a HIPAA Risk
Assessment?

POLL RESULTS

1

Yes

2

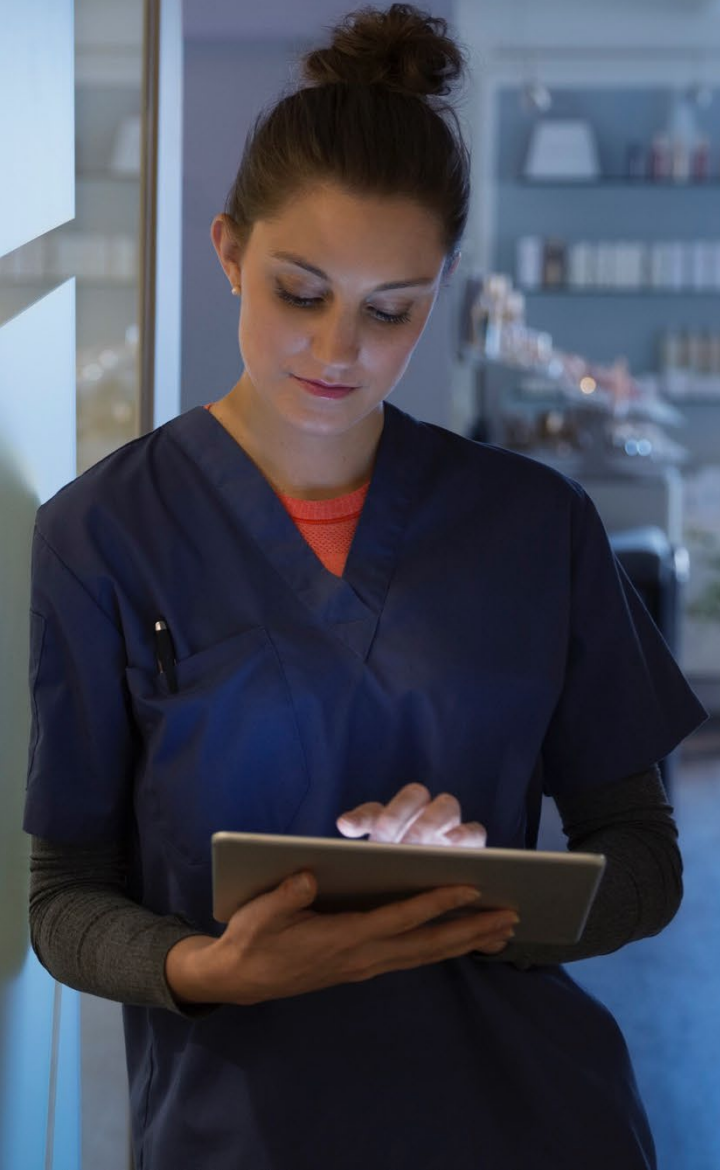
No

4

Not applicable

Building a Secure Healthcare Organization

- ▶ Start by assessing your current cybersecurity posture & identify critical cyber risks and their impact leveraging an industry leading cybersecurity framework such as NIST CSF, ISO 27001, HICP, etc.
- ▶ Develop a comprehensive cybersecurity strategy and roadmap tailored to your organization
- ▶ Establish a top-down security culture and prioritize cybersecurity as a critical business priority
- ▶ Prioritize allocation of resources across people, process and technologies areas to implement cybersecurity strategy



DISCUSSION QUESTION #3

Does your organization have a third-party risk management program?

- 1 Yes
- 2 No
- 3 Not sure
- 4 Not applicable

DISCUSSION QUESTION #3

Does your organization keep track of the latest emerging Cybersecurity risks in healthcare industry?

POLL RESULTS

1

Yes

2

No

4

Not applicable

Building a Secure Healthcare Organization

Other Resources

- ▶ NIST CSF
- ▶ Health Industry Cybersecurity Practices (HICP)

Recommended cybersecurity practices in healthcare

- ▶ Regular organizational and third-party risk assessments
- ▶ Periodic Vulnerability Assessments and Penetration Testing (VAPT)
- ▶ Minimize infrastructure and application sprawl
- ▶ Conduct periodic Cybersecurity security trainings for employees and contractors
- ▶ Implement strong data security controls including access controls, authentication methods and encryption
- ▶ Up to date system patching and inventory
- ▶ Perform and test Data back-ups periodically
- ▶ Developing and testing cybersecurity incident response plans

Recommended cybersecurity technologies and tools

- ▶ Encryption (sensitive data-at-rest and data-in-motion, DLP)
- ▶ Multi-factor Authentication (MFA) & Privileged Access Management (PAM)
- ▶ Network security solutions (i.e. IDS, IPS, WAFs, SIEM)
- ▶ Endpoint protection (Anti-virus, anti-malware)
- ▶ Email Security

Source: <https://hphcyber.hhs.gov/performance-goals.html>

Source: Healthcare and Public Health (HPH) Cybersecurity Performance Goals (CPGs)

Building a Secure Healthcare Organization

Other Resources

- ▶ NIST CSF
- ▶ Health Industry Cybersecurity Practices (HICP)

Source: <https://hphcyber.hhs.gov/performance-goals.html>

BASIC CYBERSECURITY GOALS


Mitigate known vulnerabilities


Email Security


Multi-Factor Authentication


Basic Cybersecurity Training


Strong Encryption


Revoke Credentials Timely


Basic Incident Response and Planning



Unique Credentials


Separate User and Privileged Account


Vendor/Supplier Cybersecurity Requirements

ENHANCED CYBERSECURITY GOALS


Asset Inventory


Third-Party Vulnerability Disclosure



Third-Party Incident Reporting


Cybersecurity Testing


Cybersecurity Mitigation


Detect and Respond to Relevant Threats and Tactics, Techniques, and Procedures


Network Segmentation


Centralized Log Collection


Centralized Incident Planning and Preparedness


Configuration Management

DISCUSSION QUESTION #4

Does your organization keep track of the latest emerging Cybersecurity risks in healthcare industry?

1

Yes

2

No

3

Not sure

4

Not applicable

DISCUSSION QUESTION #4

Does your organization have a third-party risk management program?

POLL RESULTS

1

Yes

2

No

4

Not applicable

Regulatory Updates

▶ HIPAA Updates -

- Analytics/ Pixel tracking:
www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html
- Release of NIST CSF 2.0 (Feb 2024):
www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework
- Change Health breach and industry-wide impact

▶ AI Legislation

- ▶ White House Minimum Standards on Cybersecurity
- ▶ FTC Updates to Health Breach Notification Rule
- ▶ NY Cyber Security Legislation
- ▶ Other Regulatory Updates:
 - SNF Staffing Mandates
 - 340B Administrative Dispute Resolution Final Rule

Questions?



DISCUSSION QUESTION #5

Would you like to speak to someone from our cybersecurity practice?

1

Yes, I would like to speak to someone from BDO

2

No, Thank You

DISCUSSION QUESTION #5

Would you like to speak to someone from our cybersecurity practice?



Yes, I would like to speak to someone from BDO.

**DO NOT DISPLAY
POLL RESULTS**



About BDO USA

At BDO, our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes — for our people, our clients and our communities. Across the U.S., and in over 160 countries through our global organization, BDO professionals provide assurance, tax and advisory services for a diverse range of clients.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C, a Virginia professional corporation, 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.

www.bdo.com

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

© 2024 BDO USA, P.C. All rights reserved.

