COLLEGE of AMERICAN PATHOLOGISTS

Cybersecurity

Preparedness and Response

Moderator: Karim Sirgi, MD, MBA, FCAP

Subject Matter Experts:

Elizabeth Sullivan, Attorney
Emily Johnson, Attorney
Jeff Christinson, MHS, PA(ASCP)
Jonathan Myles, MD, FCAP

July 23, 2024

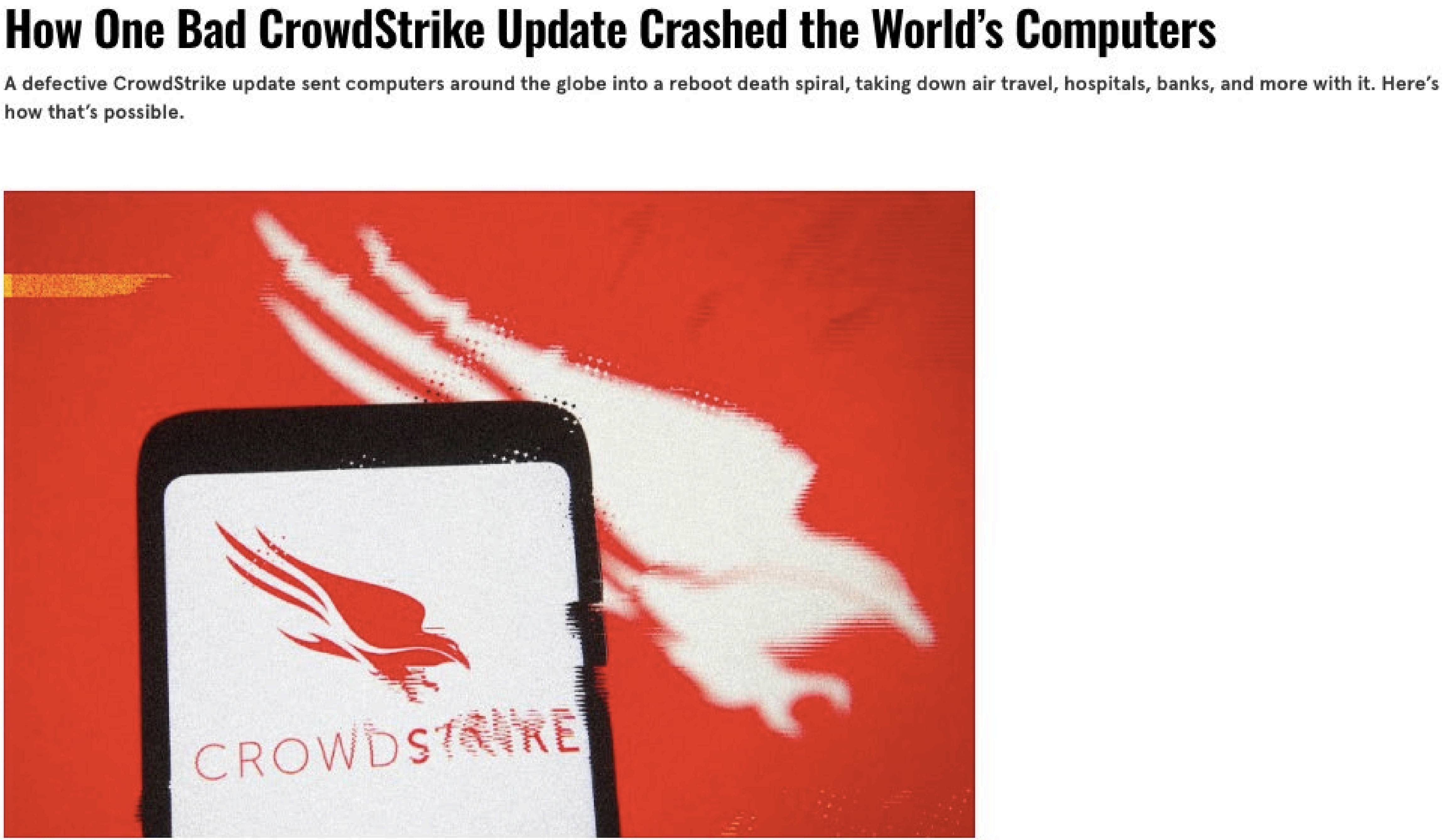
Karim E. Sirgi, MD, MBA, FCAP

- Chair – Practice Management Committee
- Owner - CEO Sirgi Consulting LLC Denver, CO
- Chair, Colorado Delegation to CAP House of Delegates
- Past-President, CAP Foundation
- Board certified AP/CP and Cytopathology
- Fellowships in Cytopathology and Surgical Pathology

Recrudescence of Attacks by Bad Players

9 reasons why healthcare is the biggest target for cyberattacks

… But Also Inadvertently by Good Players



How One Bad CrowdStrike Update Crashed the World's Computers

A defective CrowdStrike update sent computers around the globe into a reboot death spiral, taking down air travel, hospitals, banks, and more with it. Here's how that's possible.

Disclaimer

The information presented today represents the opinions of the panelists and does not represent the opinion or position of the CAP.

This should not be used as a substitute for professional assistance.

The information in this presentation is provided for educational purposes only and is not legal advice.

Jeff Christinson, MHS, PA(ASCP)

- Member – Practice Management Committee
- Chief Executive Officer for Summit Pathology, a pathologist-owned practice and laboratory that serves Colorado, Wyoming, and Nebraska.
- Graduate of Westmont College with a BA in English and a Master's of Health Science degree as a Pathologists' Assistant from Quinnipiac University.
- Since 1991, has worked for pathologist-owned practices and laboratories in various roles that have taken him from the gross bench to the boardroom.

Jonathan Myles, MD, FCAP

Past member of the Board of Governors of the College of American Pathologists. Currently Vice-Chair of the College of American Pathologists Information Technology Leadership Committee and member of the Council on Government and Professional Affairs. Previous Chair of the CAP Council on Government and Professional Affairs. Prior Vice-Chair of the CAP Council on Scientific Affairs. Previous Member of the Board Finance and Investment committees. Prior Chair of the CAP Cybersecurity work group. Pathology advisor to the AMA-RUC from 2006-2017. Chair of the College of American pathologists Economic Affairs Committee from 2010-2017.

Skilled in Clinical Research, Medical Education, Oncology, Medicine, and Quality and Patient Safety. Strong healthcare services professional with a Doctor of Medicine (M.D.) focused in Medicine from Medical College of Ohio.

Elizabeth Sullivan, Attorney

- Chair, Healthcare Practice Group
  McDonald Hopkins LLC
- esullivan@mcdonaldhopkins.com
- 248.220.1355

Emily Johnson, Attorney

- Member, Healthcare Practice Group McDonald Hopkins LLC
- ejohnson@mcdonaldhopkins.com
- 216.348.5838

Jeff Christinson, MHS, PA(ASCP)
CEO for Summit Pathology

(Painful) Feedback and (Valuable) Lessons Learned from Recent Experiences

Objectives

- Emphasize the significance of cybersecurity in healthcare
- Provide an overview of how cybersecurity is managed at the CAP, including key program components
- Discuss future cybersecurity trends and considerations for laboratories

Cybersecurity Quotes

“There are only two types of companies: those that have been hacked, and those that will be.”

- Robert S. Mueller
Former Director of the FBI

“Security is always too much until its not enough”

- **Robbie Sinclair**
Head of Security, Country Energy,
NSW Australia

“By failing to prepare, you are preparing to fail”

- Ben Franklin

““If you’re standing still in cyber, you’re getting left behind”

- Mark Johnson
CISO Hackensack Meridian Health

Cybersecurity in Healthcare

In healthcare, cybersecurity must:

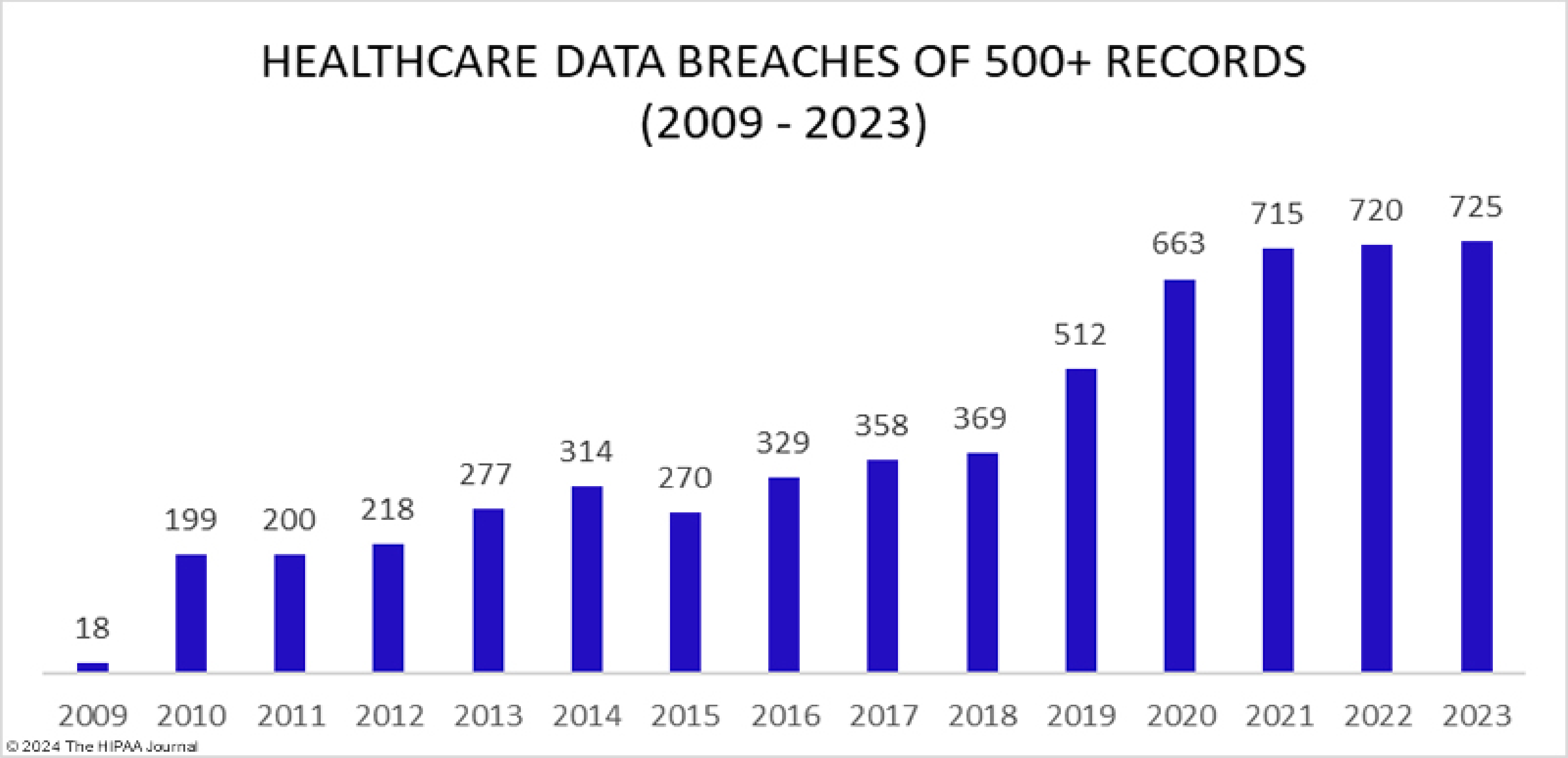
- **Protect sensitive information and systems from digital attacks and unauthorized access**
- **Ensure the safety of patient records, medical devices, and other critical systems**
- **Maintain resiliency of critical systems**
- **Ensure compliance with laws and regulations (eg, HIPAA, PCI, GDPR)**
- **Be proactive!**

"Just like we take steps to prevent infections in patients by using sterile equipment and practices, a cybersecurity program protects patient data and our healthcare systems from digital threats. This ensures that we can continue to provide care effectively, keep patient information secure, and comply with legal requirements."

- Physician cybersecurity | American Medical Association (ama-assn.org)

Rise in Healthcare Data Breaches

- The sensitive data housed by healthcare institutions, includes names, addresses, social security numbers, and medical records. This makes healthcare institutions more appealing for cybercriminals.
- This data can be more valuable on the black market than credit card information, yielding 10 to 100 times the price.

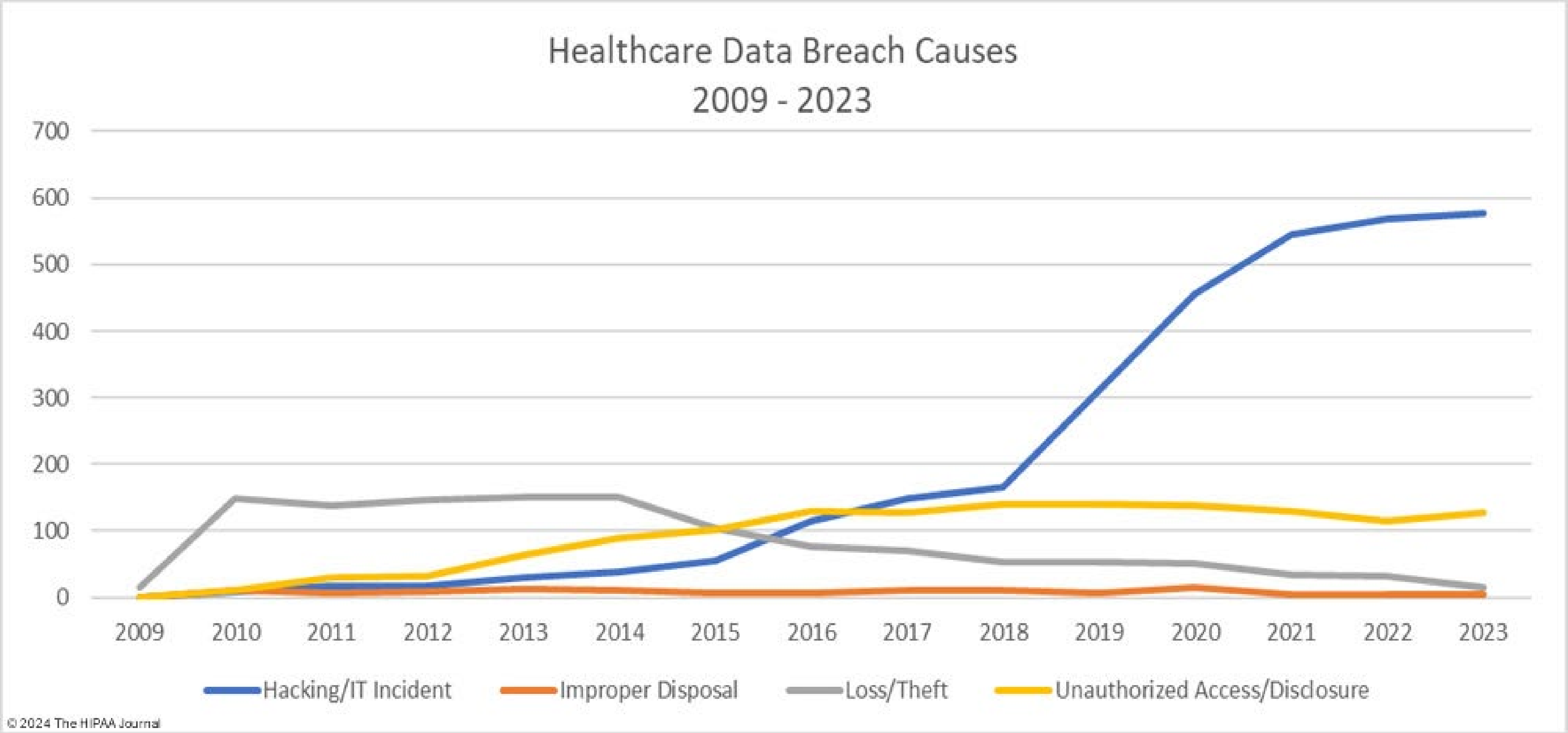


© 2024 The HIPAA Journal

- The HIPAA Journal: January 31, 2024; "Security Breaches in Healthcare 2023"
- Healthcare Data Breaches: A Rising Threat and Strategies for Prevention

Healthcare Data Breaches

- There are four times as many hacking incidents reported in 2023 than all other breach causes combined.



- The HIPAA Journal: January 31, 2024; “Security Breaches in Healthcare 2023”
- Healthcare Data Breaches: A Rising Threat and Strategies for Prevention

Cybersecurity Considerations for Healthcare (1/2)

- A cybersecurity program can and should be used to manage and mitigate cyber risks
- These programs can be guided by various frameworks and standards to ensure that effective security practices are implemented
  - It is important to select a framework which fits the needs of the organization
  - Seek to demonstrate good security defense capabilities by obtaining certain certifications such as HITRUST or SOC2
- Continuous assessments are utilized to provide visibility into the program effectiveness and risks
  - Assessments help organizations understand the effectiveness of the controls put in place to manage risk
  - Understand your risks and prioritize remediation efforts based on criticality and impact
  - Manage risks centrally using a unified solution to help prioritize, manage and maintain these risks
- The cybersecurity program should align with organizational goals and objectives

Cybersecurity Considerations for Healthcare (2/2)

- Cyber-awareness
  - Provide awareness of common threats and how to protect patients & patient data
  - Educate staff on regulatory compliance (HIPAA)
  - Reduces human error which can lead to cyber incidents
- Incident preparation
  - Business continuity – Need to maintain operations even if LIS systems are incapacitated
  - Disaster recovery – Determine how will we recover, what will we recover and in what time-period?
  - Incident response – Maintain an incident response plan and consider an incident response retainer service
- Use metrics to help gauge cybersecurity maturity and ultimately aid in decision making
- Be resourceful – Be aware of recent cyber-trends, threats and incidents and LEARN from them. Cyberattacks and Cybersecurity in… | College of American Pathologists (cap.org)

Cybersecurity at the CAP

- *How we protect the CAP*
- *What our cybersecurity strategy entails*
- *What elements make a successful cybersecurity program*

mosome abnormalities
tified by microarray
identify chromosome gains/lo es
d copy-neutral loss of hete ygosity
OH) throughout the e. -> These
anges may py
yotyping.
CAP
CAP24

CAP Cybersecurity 'In a Nutshell'

Cybersecurity at the CAP exists to:

- assess, prioritize, and mitigate risks at the CAP
- monitor and remediate threats around the clock
- ensure staff are trained and prepared
- ensure CAP complies with relevant regulations and legislation

CAP’s Cybersecurity Strategy

- ## Overview of Cybersecurity Strategy

  “Outlines key cybersecurity objectives across three themes and nine focus areas and includes metrics to improve the security of CAP's digital assets and information"

- ## Cybersecurity Mission Statement

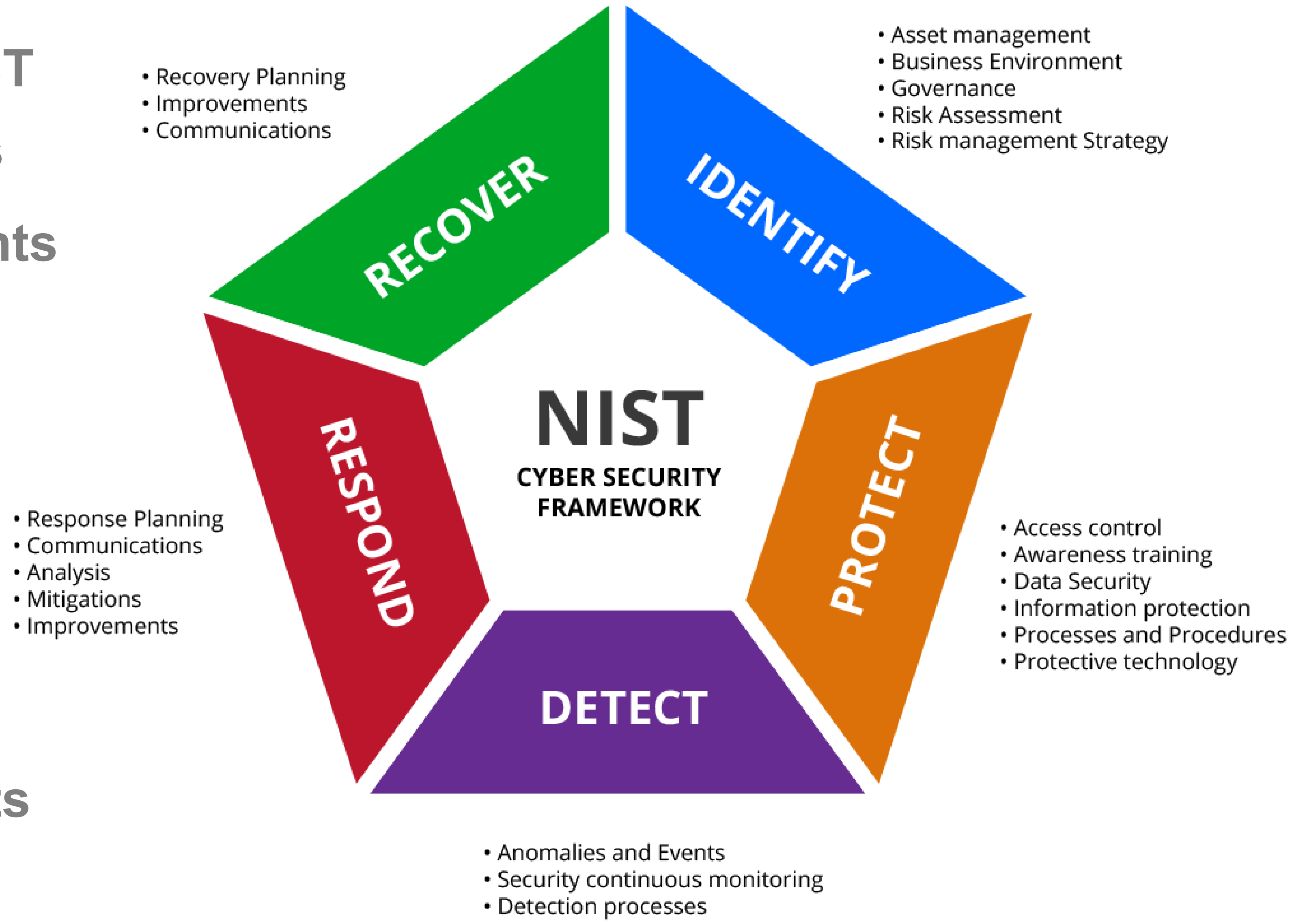
  “To partner with the CAP business to identify, prioritize, and remediate business and technology risks associated with information systems, identities, and data assets by providing security expertise, creating and maintaining resilient and secure infrastructure and solutions, and fostering a culture of security awareness and compliance throughout the organization”

- ## Strategic Themes

  - *Foster an engaged cybersecurity culture*
  - *Defend existing digital assets and information from present and anticipated threats*
  - *Support business growth and innovation initiatives by refining and expanding rings of defense*

Components used at the CAP for a Successful Cybersecurity Program

- The CAP program is based on the NIST framework, which has 5 key functions
- Within these functions are key elements to run a successful program:
    - Risk Management Strategy
    - Vulnerability Management (Attack Surface)
    - Security Incident and Event Management
    - Governance and Compliance
    - Third Party Risk Management
    - End Point Protection
    - Awareness and Training
- A robust Cyber-Insurance policy exists



- Recovery Planning
- Improvements
- Communications

- Asset management
- Business Environment
- Governance
- Risk Assessment
- Risk management Strategy

- Response Planning
- Communications
- Analysis
- Mitigations
- Improvements

- Access control
- Awareness training
- Data Security
- Information protection
- Processes and Procedures
- Protective technology

- Anomalies and Events
- Security continuous monitoring
- Detection processes

Trends and Resources

- *Cybersecurity outlook and predictions*
- *Key take-aways*
- *Resources you can access*

Future Cybersecurity Trends*

- Rise of Governance
  - Security frameworks require risk management and accountability from board members
  - Cyber insurance is stepping up their underwriting process
- Increased Attacks on Cloud Security
  - Cloud infrastructures tend to have less security than on-premise systems; easier to exploit
- Continued Threats from 'Nth' Party Vendors
  - Organizations need to consider how threats from vendors across their supply chain may affect them
- Increased Ransomware Attacks
  - More RaaS tools (Ransomware as a Service) and an insurance industry paying extortions
- Frictionless Authentication
  - Rise in ‘passwordless’ authentication (not safe to save in browsers, password vaults, etc.)

** Research and predictions sourced from Halock’s Quarterly Security Briefing with the CAP 04/25/2024*

Key Takeaways

- Cyber threats in healthcare continue to rise so we must protect sensitive information, ensure safety of our patients, maintain resiliency to critical systems, and maintain compliance
- Use a structured approach to manage your cybersecurity program
- Understand your current and future attack surface and how to manage it to an acceptable level
- Manage and prioritize risks centrally
- Obtain cyber-insurance and consider an incident response retainer should you ever need immediate help and guidance from experts
- Be proactive and prepared
- ‘Cybersecurity is a journey, not a destination’

https://www.forbes.com/sites/forbestechcouncil/2022/07/12/cybersecurity-is-a-journey-not-a-destination/

Legal Considerations

- “Breach” is ***presumed*** if:
  - Impermissible acquisition, access, use or disclosure of
  - Protected Health Information (PHI)
  - Unless CE or BA demonstrates a low probability that PHI has been compromised
    - Based on risk assessment of 4 factors
      (1) Nature & extent of PHI involved
      (2) Unauthorized person who used PHI or to whom disclosure was made
      (3) Whether PHI was actually acquired/viewed
      (4) Extent to which risk to PHI has been mitigated

Legal Considerations (cont.)

- **Avoid using the B word!!**
  - Using “breach” to describe a data-privacy related incident assumes the incident meets the definition of a security breach which triggers various notification requirements
  - An “incident” does not always rise to the level of “breach” (i.e., encryption safe harbor)
  - “Incident” is better received by the public than “breach”

Legal Considerations (cont.)

- How to protect your entity from a vendor/subcontractor breach
  - Covered Entity-Friendly Contractual Considerations:
    - Notification of Breach
      - Limit the notice period (5-10 days is standard)
    - Indemnification
      - Obligate the vendor to indemnify for any damages
    - Insurance
    - Damages
      - *"Claims, losses, liabilities, costs, fines, penalties and other expenses (including, without limitation, reasonable attorneys' fees)"*

Legal Considerations (cont.)

- Covered Entity-Friendly Contractual Considerations (cont.):
  - Compliance with data privacy standards for the protection of PII, PHI and/or PCI
  - Return or destruction of PII, PHI and/or PCI
  - Mitigation
    - *"The breaching party shall mitigate, and shall be responsible for any and all damages associated with responding to, any security incident, or related harmful effects that arise out of the acts or omissions of Business Associate, any subcontractor, or any of their officers, directors, employees"*

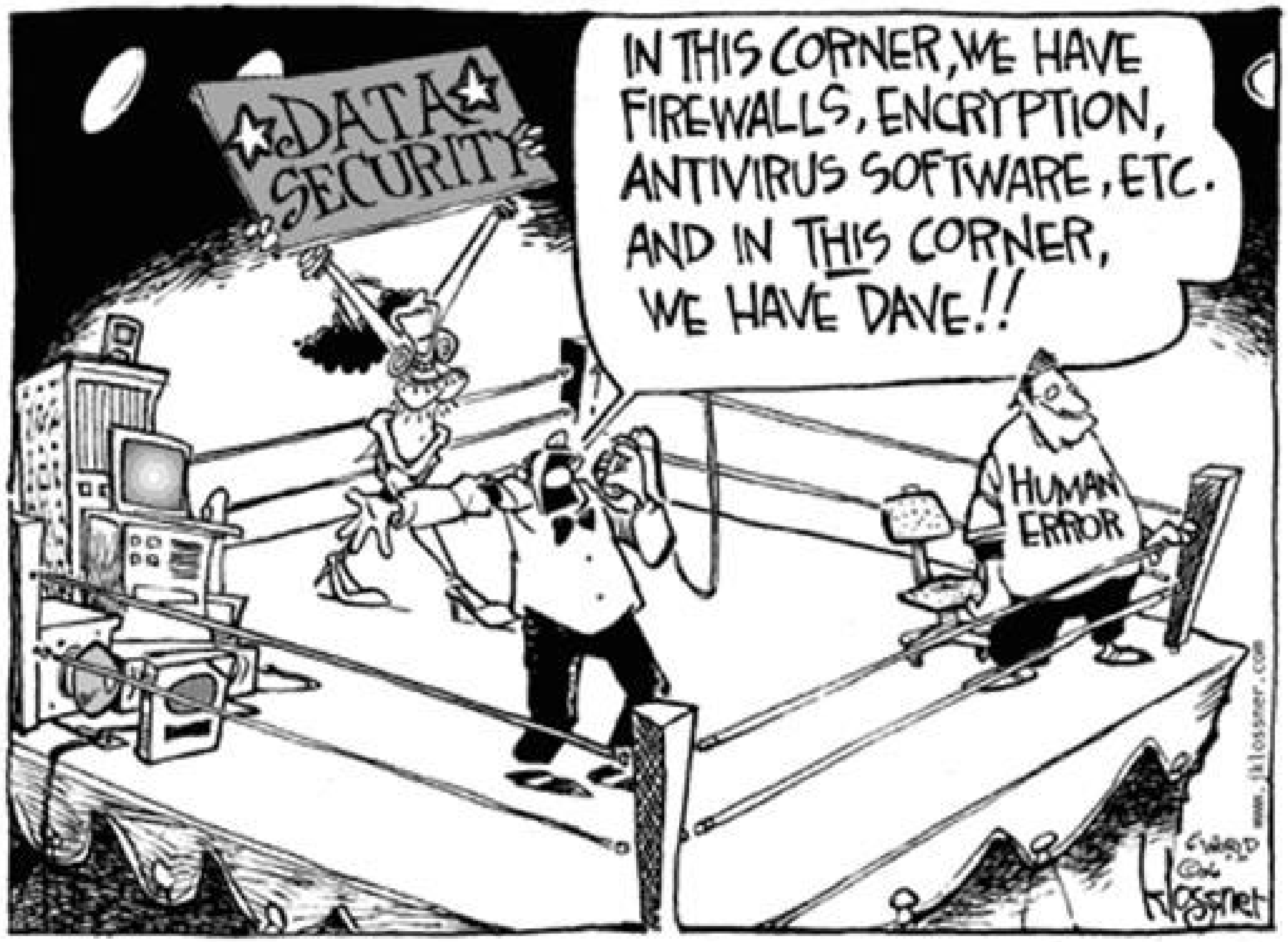
Legal Considerations (cont.)

- Practical Advice for Engaging Subcontractors
  - Ask for copies of their policies and procedures
  - Confirm they have cyberliability insurance and sufficient coverage amounts
  - Send security questionnaire to gauge compliance
  - Require risk analyses and request copies of completed risk analyses
  - Prohibit offshoring PHI
  - Limit right to subcontract without consent/notification

Legal Considerations (cont.)

- **Business Associate-Friendly Contract Considerations:**
  - Notification
    - Push out the notice period to allow for a thorough investigation
    - Business Associates technically have 60 days to notify Covered Entities of a breach
  - Indemnification
    - Beware! Indemnification provisions can impact insurance coverage
  - Mitigation
  - Right to keep information upon termination if necessary
  - Obligate Covered Entity to comply with Minimum Necessary Rule

Preventing an Incident


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©WKD 06
Klossner

Preventing an Incident

- A Written Information Security Program (WISP)
  - Required by **Massachusetts** law, **GLBA** and **FTC Red Flags Rule**
- Incident Response Plan
  - Required by **PCI DSS, GLBA** and **HIPAA**
- Carefully drafted **Confidentiality Agreements** for employees, vendors and visitors
- Proper and ongoing **training** of employees on company's data security programs
- Perform a data privacy review & **risk assessment**, including penetration testing
- Review your **employee exit** process

Links to Resources

- Cybersecurity frameworks – Consider one of these popular frameworks to help manage your security program:
  - NIST (National Institute of Standards and Technology) - https://www.nist.gov/cyberframework
  - HITRUST - https://hitrustalliance.net/hitrust-framework
  - CIS (Center for Internet Security) - https://learn.cisecurity.org/cis-controls-download
  - ISO (International Standards Organization) - https://www.iso.org/standard/73906.html
- HIPAA Security Risk Assessment Tool – This tool helps assess your organization's security posture in conjunction to the HIPAA Security Rules:
  - https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool
- Cybersecurity & Infrastructure Security Agency (CISA) – Provides tools, resources and training for the Healthcare and Public Health (HPH) sector:
  - https://www.cisa.gov/topics/cybersecurity-best-practices/healthcare

CYBERSECURITY IS

YOUR

RESPONSIBILITY TOO!

What Questions Can We Answer for You?

Elizabeth Sullivan
Attorney

Emily Johnson
Attorney

Jeff Christinson, MHS, PA(ASCP)

Jonathan Myles, MD, FCAP

Membership

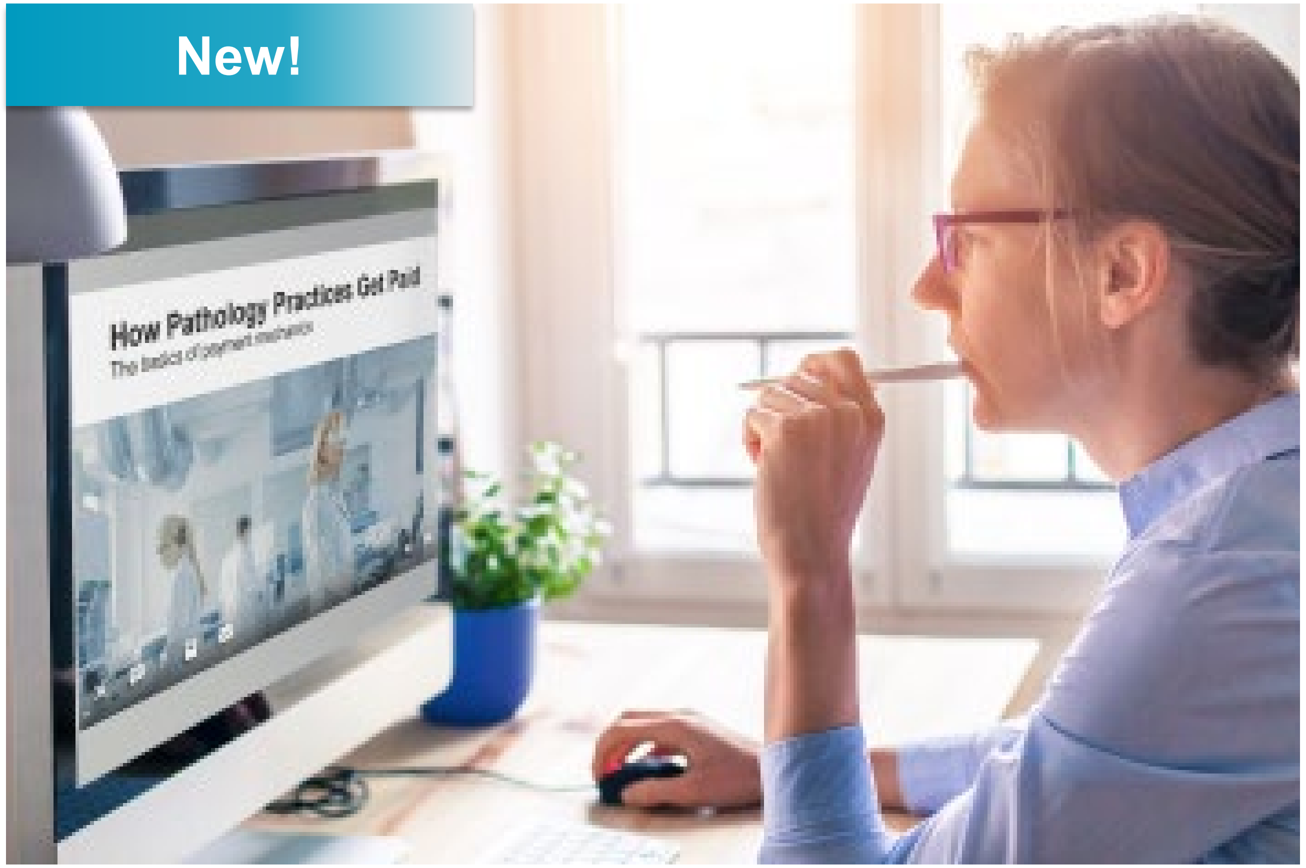
Did you find this information useful?

This program was funded by your CAP membership. Please be sure to keep your membership current so we can continue to bring timely and relevant resources like this to you.

Visit cap.org to renew your membership or email membership@cap.org.

Pathology Business Fundamentals

Essential online courses to help grow your management skills to lead your practice



1. Relative Value Units (RVU’s)—Understanding the Basics
2. How Pathology Practices Get Paid
3. Revenue Cycle Management
4. Analysis and Interpretation of Billing Reports
5. Basic Practice Cost Analysis
6. Capacity Management and Workflow Analysis
7. Basic Contracting and Fee Analysis
8. Basic Budget Development

Learn more
and register

Additional Resources

- Practice Management Webpage
  - https://www.cap.org/member-resources/practice-management
- Previous and Upcoming Roundtables/Webinars
  - https://www.cap.org/calendar/webinars/listing/practice-management-webinar
- Articles Authored by Members of the CAP Practice Management Committee
  - https://www.cap.org/member-resources/articles/category/practice-management
- Practice Management Networking Community
  - https://www.cap.org/member-resources/practice-management/practice-management-networking-community-application
- Practice Management Frequently Asked Questions
  - https://www.cap.org/member-resources/practice-management/frequently-asked-questions

Starting a New Job?

Join the Job Prep Bootcamp December 2024 for a fast-paced interactive review of cases and panel discussions on professional development courses.

Learn More

We value your feedback!

If after attending this discussion and later you applied any of what you learned to your practice, please share your feedback of how it worked for your practice at https://www.cap.org/member-resources/practice-management/practice-management-inquiry-form .

Watch for the session evaluation form. Your feedback is important!