Navigating the Changing Cyber Security Landscape

Healthcare Regulatory Roundup – Episode #66

March 6, 2024

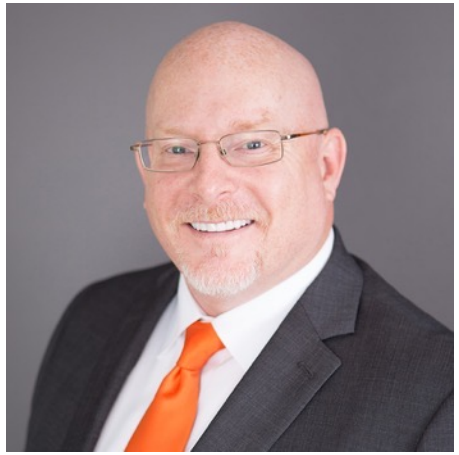
Presented by:

Barry L. Mathis, Principal | PYA

Agenda

1. Introduction
2. In The News
3. Recent Changes to Cyber Security Landscape
4. Where to Start: Elevate Your Cyber Security Risk Management
5. The Future of Cyber Security in Healthcare
6. Q&A

Introductions



Barry Mathis
Principal, PYA, P.C.
bmathis@pyapc.com

Barry has three decades of experience in the information technology (IT) and healthcare industries as a CIO, CTO, senior IT audit manager, and IT risk management consultant. He has performed and managed complicated HIPAA security reviews and audits for some of the most sophisticated hospital systems in the country. Barry is a visionary, creative, results-oriented senior-level healthcare executive with demonstrated experience in planning, developing, and implementing complex information-technology solutions to address business opportunities, while reducing IT risk and exposure. He is adept at project and crisis management, troubleshooting, problem solving, and negotiating. Barry has strong technical capabilities combined with outstanding presentation skills and professional pride. He is a prudent risk taker with proficiency in IT risk management, physician relations, strategic development, and employee team building.

Cyber Security In The News

Change Healthcare

- The attack occurred on February 21 and prompted Change Healthcare to shut down its systems, resulting in a nationwide prescription processing outage.
- More than 100 Change Healthcare applications across pharmacy, medical record, clinical, dental, patient engagement, and payment services were affected, the company said in an 8-K filing with the SEC (Securities and Exchange Commission).
- As of March 5, however, Change Healthcare has not been able tor restore the affected systems, according to an update to UnitedHealth's incident notification.

AHA Bulletin

In The News

APT29 Cozy Bear

- The Russian intelligence hacking group known as APT29 or Cozy Bear is responding to the corporate migration to the cloud with matching hacking techniques, says an alert from international cyber agencies.

- Threat intelligence firms warn that APT29 has amplified its global cyberespionage operations.

- The group uses techniques such as brute-forcing the password of dormant accounts or service accounts used to make automated API calls. Service accounts are desirable targets because they typically lack multifactor authentication, says a Monday alert from the Five Eyes intelligence alliance, which consists of the United Kingdom, the United States, Canada, Australia and New Zealand.

LockBit Relaunches Dark Web Leak Site

- In a lengthy missive, the LockBit leader said the FBI appears to have used a vulnerability, tracked as CVE-2023-3824, in web-scripting language PHP to penetrate the ransomware-as-a-service operation's servers. LockBit didn't patch the vulnerability "because for five years of swimming in money I became very lazy."

- Law enforcement did not take down backup servers that didn't have PHP installed, LockBit said.

- LockBit Statement on DarkWeb: "All FBI actions are aimed at destroying the reputation of my affiliate program, my demoralization, they want me to leave and quit my job, they want to scare me because they can not find and eliminate me, I can not be stopped, you can not even hope, as long as I am alive I will continue to do pentest with postpaid," the missive states.

In The News

Connectwise

- Hackers are aggressively exploiting unpatched ConnectWise ScreenConnect remote connection software to infect systems with ransomware, info stealers and persistent backdoors. The attacks observed by researchers include ransomware deployments tied to the now-defunct LockBit ransomware operation.

- ConnectWise is urging customers with on-premises equipment to patch two high-risk vulnerabilities affecting ScreenConnect servers and ScreenConnect clients - an entreaty that grew in urgency after security researchers published a proof of concept for an authentication bypass flaw tracked as CVE-2024-1709. The flaw has a CVSS score of 10 - the maximum possible, making it, "critical."

In The News

HHS OCR Tells Congress It Needs More Funding for HIPAA Work

- In 2022, OCR received 63,966 reports of breaches affecting fewer than 500 individuals, and unauthorized access or disclosure was the most frequently reported breach type. These smaller breaches affected 257,105 individuals.
- The breach figures for 2023, which will be reported to Congress next year, paint an even grimmer picture.
- The HHS OCR HIPAA Breach Reporting Tool website showed 739 major breaches reported in 2023 that affected more than 136 million individuals. That's an all-time record for the number of breaches reported, as well as the total number of people affected in one year.
- HHS OCR told Congress that the lack of adequate funding also has inhibited the agency's ability to carry out another mandate of the HITECH Act - performing periodic audits of covered entities and business associates to assess compliance with HIPAA rules.

Recent Changes to Cyber Security Landscape

Recent Changes to the Cyber Security Landscape

Cybersecurity and Infrastructure Security Agency

- Started in 2019 and determined to help (10 Regions)
- The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.
- The agency connects its stakeholders in industry and government to each other and to resources, analyses, and tools to help them fortify their cyber, communications, and physical security and resilience, which strengthens the cybersecurity posture of the nation.

Recent Changes to the Cyber Security Landscape

NIST Unveils Second Iteration of Cybersecurity Framework

- Cybersecurity guidance for the private sector published by the U.S. National Institute of Standards and Technology has received its first major update since its first unveiling in 2014.

- The revised Cybersecurity Framework focuses on governance and urges organizations - "from the smallest schools and nonprofits to the largest agencies and corporations" - to consider cybersecurity threats a major source of enterprise risk.

- The updated framework adds one new core element of a cybersecurity program - governance - to the five originally established in 2014: identify, protect, detect, respond and recover.

Recent Changes to the Cyber Security Landscape

Cyber Incident Reporting for Critical Infrastructure Act

- Substantial cyber incidents that are likely to result in demonstrable harm.
- Entities in 16 critical infrastructures defined in Presidential Policy Directive 21 (Includes Healthcare Providers)
- Reports go to Cybersecurity and Infrastructure Security Agency (CISA)
- Incidents reported no later than 72 hours after the affected entity reasonably believes that the covered cyber incident has occurred.
- Incidents should be reported until the cyber incident at issue has concluded and has been fully mitigated and resolved.
- Ransom payments reported to CISA within 24 hours.

Recent Changes to the Cyber Security Landscape

State and Local Cybersecurity Grant Program

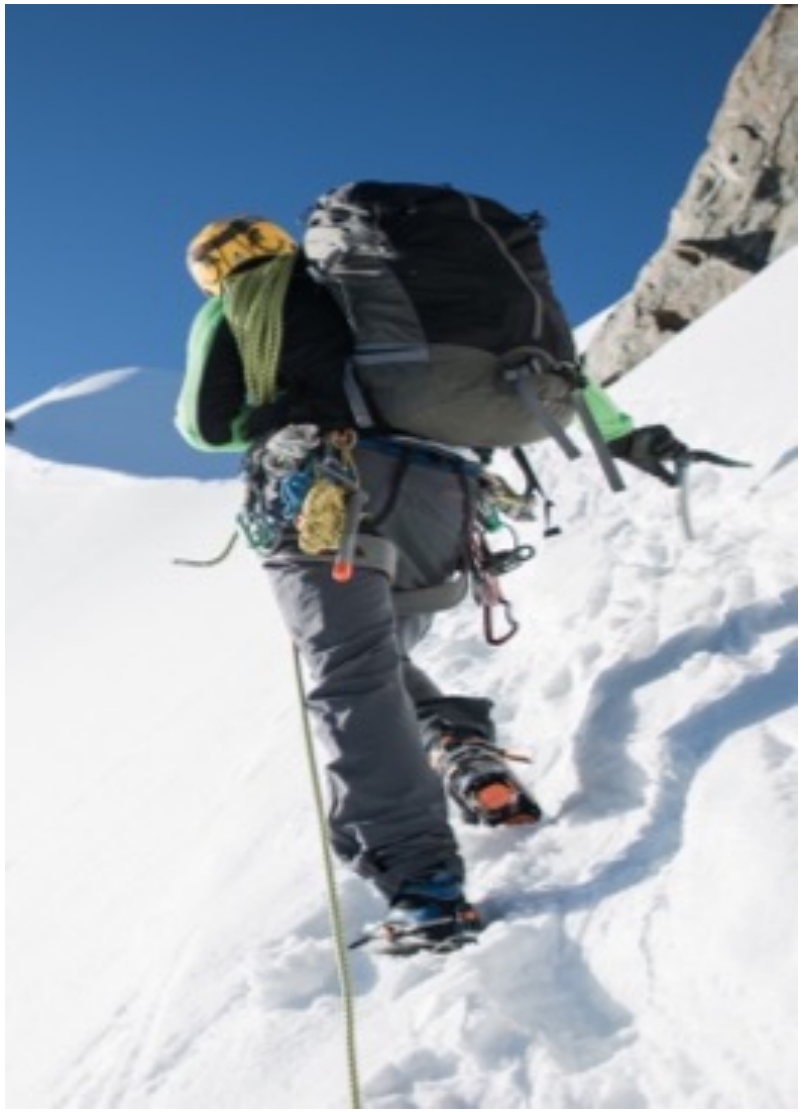
- Congress established the State and Local Cybersecurity Grant Program (**SLCGP**) to "award grants to eligible entities to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state, local, or tribal governments."
- $400 million for FY 2023, $300 million for FY 2024, and $100 million for FY 2025.
- State Administrative Agencies for states and territories are the only eligible applicants.

Elevate Your Cyber Security Risk Management

Elevate Your Cyber Security Risk Management

Start with the Basics

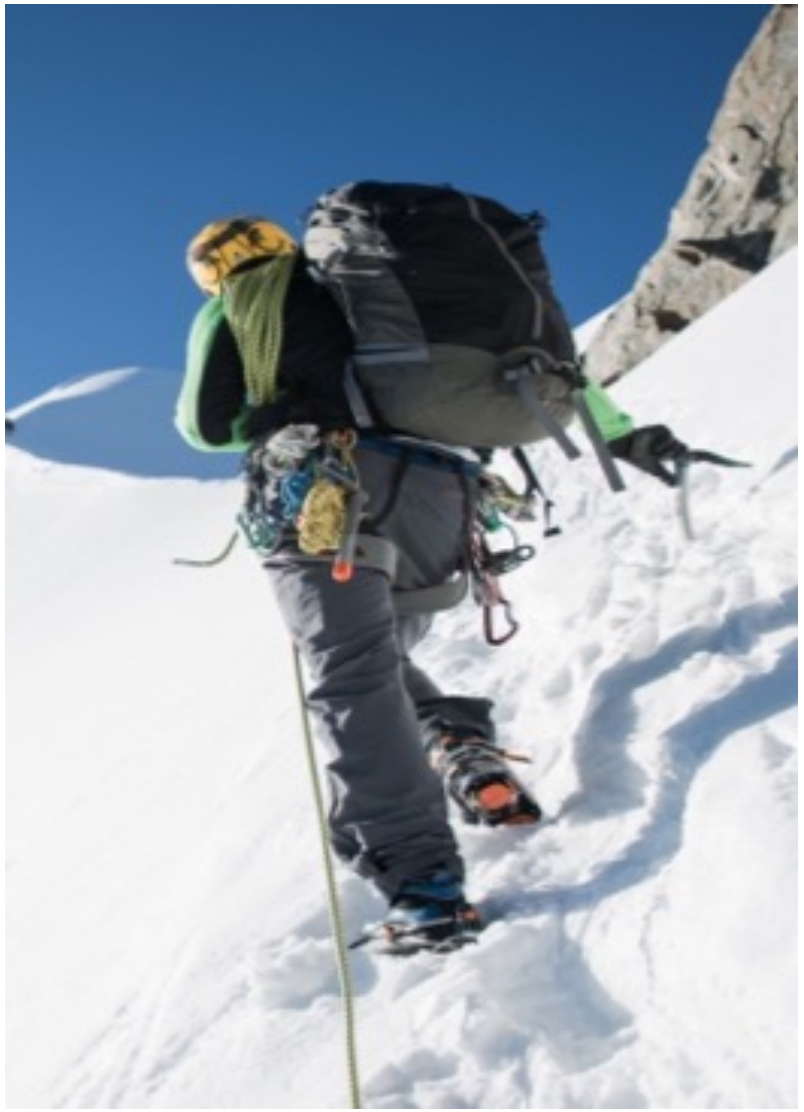
- Multi Factor Authentication is a must
- Monitoring and Logging
- Complete a Security Risk Analysis
- Mitigate known issues
- Patch Servers and Infrastructure
- Test and Train



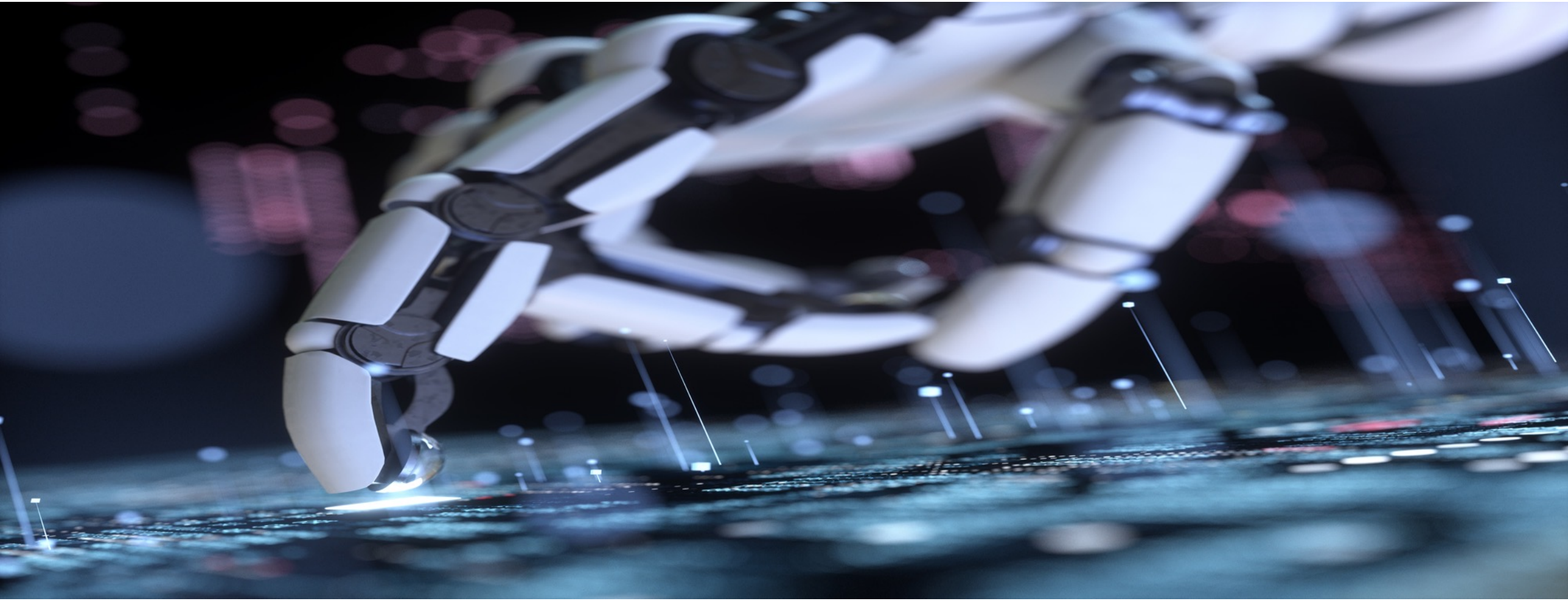
Elevate Your Cyber Security Risk Management

Start with the Basics

- Encrypt Devices
- Reduce Local Data Presence
- Build and Test Contingencies
- Incident Planning
- Test and Train, again



The Future of Cyber Security in Healthcare



The Future of Cyber Security in Healthcare

- Risks to continue into IOT and BioMed
- AI Defensive Tools
- HHS Voluntary cybersecurity performance goals
  - HHS is publishing these voluntary healthcare specific **Cybersecurity Performance Goals (CPGs)** to help healthcare organizations prioritize implementation of high-impact cybersecurity practices.
- Angler Phishing.
  - This newer form of phishing uses social media rather than email. Cybercriminals may create posts, tweets, or even instant messages that target their victims. They often refer to data mined from the target's previous posts, such as geotags or recent celebrations, which the target might not even remember they posted.

Thank you!

Barry Mathis, Principal
IT Advisory & Consulting, PYA
Bmathis@pyapc.com

pyapc.com
800.270.9629