PYA

"Critical Pathway Information Technology and How To Prepare for a Cyber Disaster"

SUMMER CPE SYMPOSIUM – SESSION #4

June 21, 2024

Summer CPE
SYMPOSIUM

WE ARE AN INDEPENDENT MEMBER OF HLB—THE GLOBAL ADVISORY AND ACCOUNTING NETWORK

Introductions

Barry Mathis

Principal

bmathis@pyapc.com

PYA

pyapc.com
800.270.9629

ATLANTA | CHARLOTTE | KANSAS CITY | KNOXVILLE | NASHVILLE | TAMPA

In the wake of the Change Healthcare cyber attack, many health systems are focused on what caused the attack. It may be more beneficial to focus on what the cyber attack caused.

Information system critical pathways represent the core processes and workflows that rely on technology to function effectively.

By identifying and understanding these pathways, healthcare organizations can better prepare for the impact of a Cyber Disaster.

Navigating Information System Critical Pathways

Form a Multidisciplinary Team

- Establish a multidisciplinary team comprising representatives from various departments, including IT, clinical, administrative, and compliance.
- Ensure that the team has a comprehensive understanding of the organization's structure, operations, and information technology landscape.

Conduct Stakeholder Interviews

- Interview key stakeholders across different departments to gather insights into the information systems they use and their interdependencies.
- Document the functionalities, workflows, and integration points of each system from the perspectives of end-users.

Review Existing Documentation

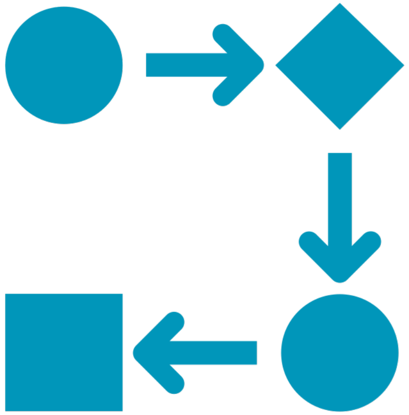
- Gather and review any existing documentation related to information systems, such as IT inventories, network diagrams, system architectures, and vendor contracts.
- Cross-reference this documentation with stakeholder interviews to validate the accuracy and completeness of the information.

Perform System Inventory

- Create a comprehensive inventory of all information systems used within the organization, including EHR systems, clinical applications, administrative software, communication tools, and third-party solutions.
- Document key attributes of each system, such as name, vendor, version, purpose, functionalities, and users.

Map Data Flows and Integration Points

- Identify the data flows and integration points between different information systems, including interfaces, APIs, data exchanges, and interoperability standards.
- Document how data is transferred, transformed, and utilized across systems to support various workflows and processes.



Collaborate with IT Department

- Work closely with the IT department to access technical documentation, system configurations, network topology diagrams, and security policies.
- Engage IT staff to provide insights into system architecture, dependencies, and maintenance processes.
- Leverage IT tools and resources, such as network monitoring software, asset management systems, and configuration management databases (CMDBs), to aid in the identification and documentation of information systems.
- Implement automated discovery tools to scan network infrastructure and identify connected devices and systems.

Document Interdependencies

- Document the interdependencies between information systems, including dependencies on hardware, software components, databases, servers, and network infrastructure.
- Identify critical pathways and points of failure that may impact the overall functioning of the healthcare organization.

Validate and Verify Information

- Validate the accuracy and completeness of the documented information through peer reviews, validation sessions, and feedback from stakeholders.
- Verify the documentation by conducting audits, walkthroughs, and inspections of information systems and their interconnections.

Maintain Documentation

- Establish a centralized repository or knowledge base to store and maintain documentation related to information systems and their interconnections.
- Implement a process for regular updates and revisions to ensure that the documentation remains current and reflective of any changes in the organization's IT landscape.

Business Contingency and Alternate Pathways

- Developing business contingencies and alternative pathways in the event of an information technology disaster is crucial for hospitals to ensure continuous patient care and operational stability.
- Having alternative pathways allows medical staff to access patient records, communicate effectively, and deliver timely treatments without relying solely on electronic systems.
- Multiple pathways ensure that financial transactions can continue even if primary systems are unavailable, minimizing revenue loss and financial instability.

Preparing for a Cyber Disaster

Risk Assessment and Management

- Conduct Regular Risk Assessments:
  - Identify and evaluate potential cyber threats, vulnerabilities, and the impact of different attack scenarios. This should include technical, operational, and organizational aspects.
- Implement Risk Mitigation Strategies:
  - Develop and deploy measures to reduce identified risks, such as encryption, access controls, and regular software updates.

Incident Response Plan

- Develop a Comprehensive Incident Response Plan:
  - Outline clear procedures for detecting, responding to, and recovering from cyber incidents. This plan should define roles and responsibilities, communication protocols, and escalation processes.
- Conduct Regular Drills and Simulations:
  - Test the incident response plan through regular drills and simulations to ensure readiness and identify areas for improvement.

Data Backup and Recovery

- Implement Robust Backup Solutions:
  - Regularly back up critical data to secure, offsite locations. Ensure backups are encrypted and protected from unauthorized access.
- Establish a Data Recovery Plan:
  - Develop and test a data recovery plan to ensure that critical systems and data can be restored quickly and effectively after a cyber incident.

Employee Training and Awareness

- Conduct Regular Training Programs:
  - Educate employees about cybersecurity best practices, common threats, and how to respond to potential incidents. Training should be ongoing and updated regularly.
- Promote a Security-Aware Culture:
  - Encourage a culture of security awareness and vigilance among staff. Employees should understand their role in protecting sensitive data and systems.

Security Technologies and Practices

- Deploy Advanced Security Technologies:
  - `Utilize firewalls, intrusion detection/prevention systems, endpoint protection, and other advanced security technologies to safeguard IT infrastructure.
- Implement Multi-Factor Authentication (MFA):
  - Require MFA for accessing critical systems and data to add an extra layer of security.
- Regularly Update and Patch Systems:
  - Ensure all software and systems are up-to-date with the latest security patches and updates to protect against known vulnerabilities.

Collaboration and Information Sharing

- Join Information Sharing Organizations:
  - Participate in healthcare-specific information sharing and analysis centers (ISACs) to stay informed about emerging threats and best practices.
- Collaborate with Law Enforcement and Regulatory Bodies:
  - Establish relationships with law enforcement agencies and regulatory bodies to facilitate timely reporting and response to cyber incidents.

PYA

A national healthcare advisory services firm
providing consulting, audit, and tax services

PYA by the Numbers

40% FEMALE OWNERSHIP

Over 2x the average of similarly sized firms

- Inside Public Accounting

Consistently ranked
TOP 20
HEALTHCARE CONSULTING
firm in the U.S.
by Modern Healthcare

TOP 15 LARGEST AUDITOR
of AHA's Top U.S. Multi-Hospital Systems
- Ames Research Group

INSIDE public accounting
BEST OF THE BEST FIRMS
2023

Clients in **ALL 50 STATES**

USA TODAY
MOST RECOMMENDED
TAX & ACCOUNTING FIRMS
2024
IN COOPERATION WITH statista

MORE THAN **3400** HEALTHCARE CLIENTS

Academic Medical Centers | Accountable Care Organizations Ambulatory Surgery Centers | Blood Centers | Clinically Integrated Networks | County Owned Hospitals | Critical Access Hospitals Diagnostic Centers | Dialysis Centers | Health Plans | Health Systems | Home Health Agencies | Hospices | Hospitals Independent Practice Associations | Maternity Centers | Medical Groups | Mental Health Centers | Nursing Homes Physician-Hospital Organizations | Physician Practices | Physical Therapy Centers | Psychiatric Hospitals | Rural Health Centers Safety Net Hospitals | Surgery Centers | Urgent Care Centers

Vision Beyond the Numbers®

We measure our success based on the success of our clients.

Our culture of HELP and helpfulness is an intrinsic daily philosophy.

RESPONSIVE

ACCESSIBLE

COMMITTED