

Cyber Resilience in Healthcare: A Critical Case Study



shoar.ai/react

Executive Summary

In the fall of 2023, a non-profit healthcare system operating across the Midwest faced a severe cybersecurity crisis. This case study examines the incident, its impact, and key lessons for enhancing cyber resilience in the healthcare sector.

Background

- **Organization:** Non-profit healthcare system
- **Scope:** 15 hospitals and facilities, including several 340B institutions
- **Location:** Midwest, United States
- **Incident:** Sophisticated ransomware attack

Incident Overview

Despite utilizing the Epic electronic health record system and believing they had adequate downtime procedures, the organization fell victim to a sophisticated ransomware attack.

The immediate impact was catastrophic, forcing the entire healthcare system to revert to paper-based operations for approximately two weeks.



Key Challenges and Impact

Operational Disruption

- Patient care continuity compromised
- Medical records management severely impacted
- Provider documentation processes disrupted
- Financial processes halted



Key Challenges and Impact

Provider Documentation

- Extended "Observation" status classifications due to incomplete/inaccurate documentation
- Prolonged revenue cycle. Potential impact on patient care decisions

Medical Records Management

- Lack of protocols for paper documentation led to inconsistent record-keeping
- Post-attack digitization resulted in a disorganized "dump" of information into Epic

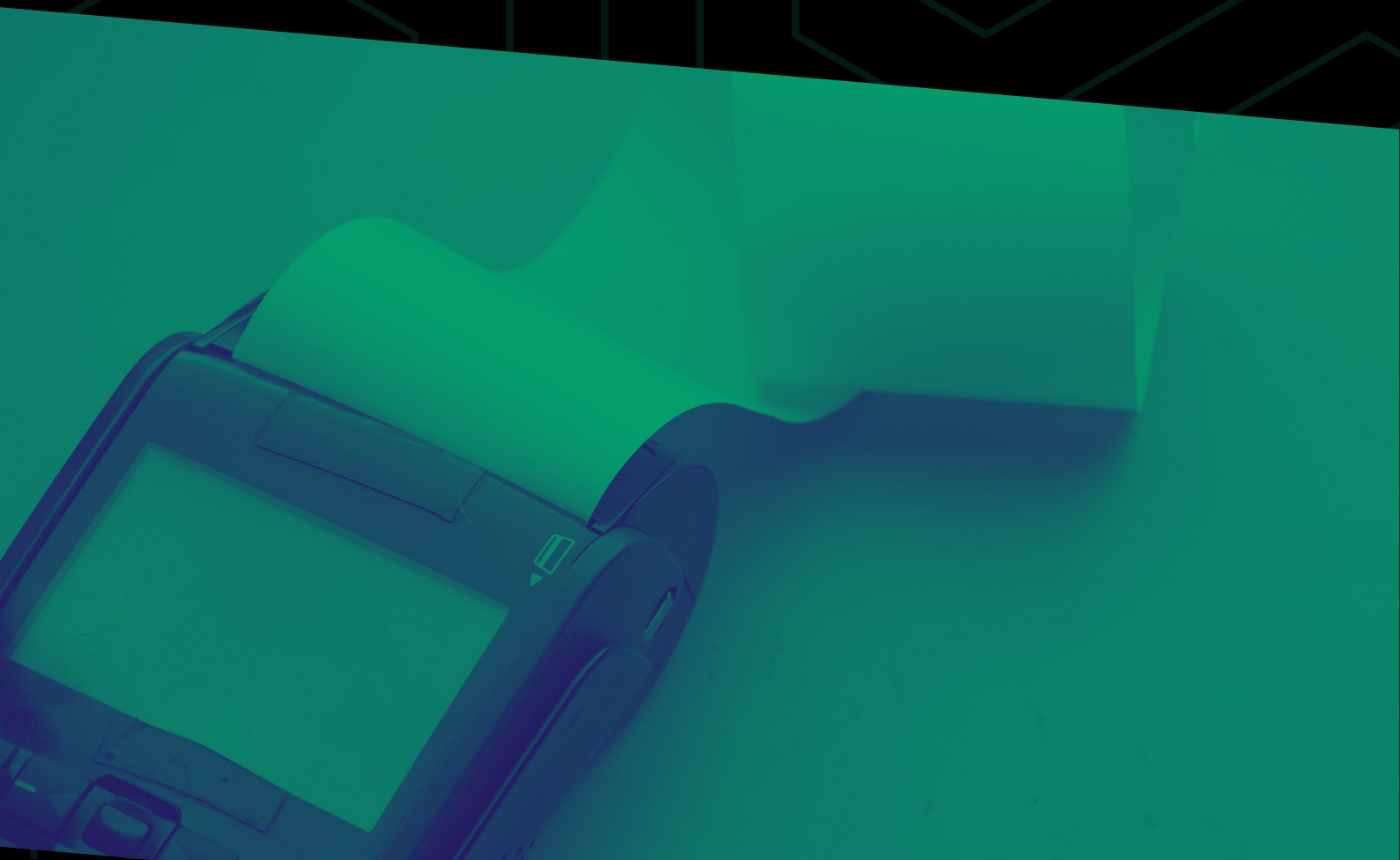
Clinical Documentation

- Non-standardized downtime procedures across departments
- Inconsistent records complicated post-attack recovery and billing accuracy

Key Challenges and Impact

Charge Capture

- Manual systems led to widespread errors in recording billable services
- Particular difficulty in reconciling Medication Administration Records for 340B facilities
- Resulted in revenue loss and claims verification complications



Financial Impact

Monthly Costs

\$500,000 to \$750,000

Total Remediation

Estimated between \$4 million and \$6.5 million
(excluding lost revenue and reputational damage)

Additional personnel

50 staff hired for 35 weeks to review claims

Payment Delays

Due to payer audits

Industry Context

- 707 major health data breaches reported in the U.S. in 2023, affecting over 112 million individuals
- Average cost of a healthcare data breach in 2023: \$10.93 million

Key Lessons

Key Lessons and Recommendations

Enhance Paper Documentation Protocols

- Develop standardized procedures for maintaining accurate records during system outages
- Conduct regular drills to ensure staff familiarity with paper-based processes

Standardize Downtime Procedures

- Implement uniform protocols across all departments
- Regularly update and communicate these procedures to all staff

Improve Manual Charge Capture Systems

- Develop robust manual systems for accurately recording billable services
- Pay special attention to complex areas like 340B facility medication administration

Strengthen Cyber Resilience Planning

- Conduct regular risk assessments and penetration testing
- Invest in advanced threat detection and response capabilities
- Implement a comprehensive incident response plan

Enhance Staff Training

- Regularly train staff on cybersecurity best practices
- Conduct simulations of cyber incidents to improve readiness

Ensure Regulatory Compliance

- Maintain compliance with healthcare regulations and data security standards during recovery
- Establish clear procedures for patient data protection during crises

Conclusion

This case study highlights the critical importance of comprehensive cyber resilience planning in healthcare.

Organizations must not only focus on robust IT systems but also on operational procedures and staff preparedness to mitigate the impact of cyber incidents effectively.

TO SCHEDULE A DEMO OR TO LEARN MORE ABOUT REACT. VISIT



SHOAR.AI/REACT

