Sponsored by:

FTI CONSULTING

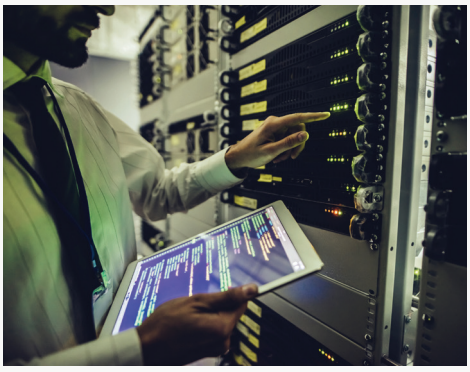
AHA TRANSFORMATION TALKS

STRATEGIES FOR REIMAGINING HEALTH CARE

Reducing Cybersecurity Risks During Digital Transformation

Ransomware attacks and cybersecurity breaches are plaguing the health care field, jeopardizing patient data and the ability to deliver safe, efficient care.

- In the first half of 2021, **health care providers reported 325 data breaches** of protected health information (PHI).[1]
- **More than one-third of health care organizations were hit** by a ransomware attack in 2020.[2]



As hospitals and health systems across the nation accelerate their digital transformation in response to the pandemic, and to take advantage of rapidly advancing technologies, they also are increasing their exposure to cyber risks.

These risks, which often are introduced through the software supply chain or other mission-critical technology, can negatively impact patient confidentiality, care delivery, safety and business operations. Potential cyber incidents can arise via human error and misconfigurations or through more malicious intent as cyber criminals seek to exploit vulnerabilities within organizational networks, third parties and the supply chain.

In national news, we often focus on cyber incidents that impact confidentiality, notably data breaches. While data breaches and other data exposure events are still serious, for health care providers, cyber incidents that impact availability and integrity can be far more serious as there are physical implications in life-saving situations, such as clinicians not being able to access critical information before making medical decisions.

American Hospital Association™
Advancing Health in America

SHSMD Society for Health Care Strategy & Market Development™

AHA CENTER FOR HEALTH INNOVATION

With the need to continue to push ahead with digital transformation while maintaining the highest safety standards, health care leaders must assess common pitfalls in this transition and carefully evaluate and implement cybersecurity risk-mitigation strategies.

Three proactive steps to take now

Assess application architectures and underlying code regularly. Third parties that supply applications, such as EHR vendors and medical device manufacturers, should be held to strict information security and data protection standards and regularly assessed for new risks. Health Care systems should incorporate cybersecurity risk into their purchase decisions.

Control networks. Tightly and continuously monitor networks for evidence of suspicious traffic. In particular, network security and access controls should be used to prevent unauthorized access to health care critical infrastructure and critical software, especially legacy systems that cannot be easily patched or securely configured by default.

Conduct regular testing. Identify gaps in security controls with regular vulnerability scanning and penetration tests against critical systems. This enables immediate remediation efforts before attackers can exploit the same weaknesses. Penetration tests should have explicit rules of engagement so as not to cause inadvertent outages to production systems and follow the tactics of known adversaries that attack health care providers.

Resources

1. Department of Health & Human Services' Office for Civil Rights Breach Portal.
2. "The State of Ransomware in Healthcare in 2021," Sophos.

To help your organization transform, visit the **AHA Transformation Talks website**.

Discussion Questions:

1. **What is the current cybersecurity threat level to hospitals and health systems; how are these threats being manifested?**
2. **What is the best way organizations can take inventory of risks to their business and monitor networks for suspicious traffic or activity?**
3. **As providers continue in their digital transformation, what third-party, supply-chain risks come into play for organizational cybersecurity? How can provider organizations predict and ideally prevent events like the SolarWinds breach in 2020?**
4. **What role should senior leaders play in engaging their information technology leaders in assessing, managing and acting upon cybersecurity risks and breaches? How often should they be briefed on these metrics?**