Crowe

Cyberrisk Checkup

Diagnosing cybersecurity risks

Issue

Cybersecurity risks in healthcare are amplified by compliance drivers, pressure from decreasing reimbursements, and a persistent call to innovate. Cybersecurity is not an IT problem or a HIPAA checklist item to complete annually – it is a dynamic element. Governance, focus, and resources are needed to protect not only the organization but also patient safety. The challenge is to understand both business strategy and IT strategy because more providers are interconnected and more services are outsourced throughout the continuum of care.

The risk landscape

more than 2,100

- Patient deaths annually can be attributed to hospital data breaches[1]

$3.7 million

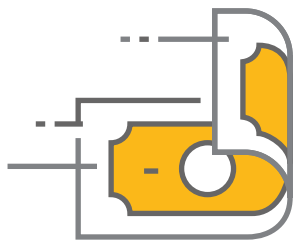
- Average lost revenue per data breach[3]

Lack of appropriate personnel

- Number one barrier of healthcare organizations to remediating and mitigating cybersecurity[2]

$6.2 billion

- Annual cost of data breaches to healthcare industry[3]



[1] https://www.beckershospitalreview.com/cybersecurity/study-hospital-data-breaches-tied-to-thousands-of-additional-patient-deaths.html

[2] "2018 HIMSS Cybersecurity Survey," Healthcare Information and Management Systems Society, http://www.himss.org/2018-himss-cybersecurity-survey

[3] "Healthcare Breaches Cost $6.2B Annually," Becker's Hospital Review, Jan. 19, 2017, https://www.beckershospitalreview.com/healthcare-information-technology/healthcare-breaches-cost-6-2b-annually.html

Action

How can you understand your cybersecurity risks, remediate or mitigate those risks, and prioritize investments to help protect your patients from harm and your organization from loss or disruption?

Crowe healthcare cybersecurity solutions can help organizations answer healthcare's toughest cybersecurity challenges and questions:

- How can we gain a better understanding of our cybersecurity risks and the gaps in our cybersecurity program?
- Would our HIPAA compliance program pass an Office for Civil Rights (OCR) audit?
- Do we know what's on our network?
- Could we be hacked, what would be the impact, and would we even know we had been hacked?
- Are our medical devices secure?
- How susceptible are we to phishing attacks against our users?
- Do our vendors expose us to significant cybersecurity risk?
- Do we have enough staff to execute our cybersecurity program?

Crowe solutions cover a broad range of cyberrisks and offer a holistic approach to helping you assess risks, remediate problems, and maintain measures to help protect your organization and address compliance expectations. Our solutions include:

- Cybersecurity assessments
- HIPAA compliance
- IoT security
- Penetration testing
- Medical device risk management
- Network device visibility and intelligence
- Security awareness and phishing
- Third-party risk management
- Virtual information security office

Crowe offers excellence in cybersecurity services:

- A national practice with more than 200 cybersecurity specialists
- Specialists accredited with multiple technical security certifications including CISSP, HCISPP, CEH, OSCP, OSCE, CCSFP, and CISA
- Full access to suites of commercial and noncommercial innovative tools built in our cybersecurity labs

In addition, the firm is active in the cybersecurity community and is a frequent sponsor of the National Collegiate Cyber Defense Competition. Crowe cybersecurity specialists also have served as speakers at Black Hat, DEF CON, and DerbyCon cybersecurity conferences.

For more information please contact:

Raj Chaudhary
Principal
+1 312 899 7008
raj.chaudhary@crowe.com

Jared Hamilton
+1 317 706 2724
jared.hamilton@crowe.com

Candice Moschell
+1 317 208 2456
candice.moschell@crowe.com

HC-19005-019A