Symantec.

As risk management matures, cybersecurity gaps still loom

Healthcare's approach to cybersecurity is maturing, but not quickly enough. The third annual HIMSS Analytics IT Security and Risk Management Study[1] showed improvements in risk management. However, there are still gaps with addressing increasing security threats and evolving concerns around the risks of medical devices and cloud adoption.

Cybersecurity is an enterprise-wide concern.

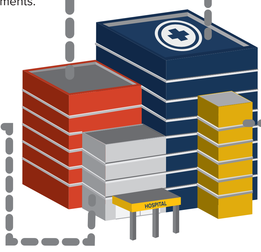
Healthcare organizations are beginning to implement practices that demonstrate a more mature understanding of cybersecurity as an enterprise-wide concern. Cybersecurity is no longer considered solely an IT responsibility or a compliance issue.

60% of healthcare providers are now identifying risk assessment, rather than HIPAA compliance, as the #1 driver for security investments.

8 of 10 providers provide a cybersecurity brief at Board meetings (though half of these respondents claim it is still on an ad-hoc basis).

More providers have adopted cybersecurity frameworks, with

40% using more than one framework.



- 63% NIST CSF
- 37% HITRUST
- 31% ITIL

are the top three most commonly adopted frameworks.

59% of respondents identified "performance against risk frameworks" as a top security KPI.

Healthcare providers need more resources to combat obstacles.

Despite this progress, providers still struggle with getting enough resources to combat the continually evolving threat landscape.

In 2017 alone, the Office of Civil Rights, in the U.S. Department of Health and Human Services, reported

358 HEALTHCARE PROVIDERS suffered a breach of **500+** RECORDS

These reported breaches affected a total of

5,136,438 individuals.[2]

73% of providers identified "budget" as the most significant barrier to improving their security programs, with "staffing" and "skillsets" coming in 2nd and 3rd.

74% of providers devote 6% or less of their total IT budget to IT security. In fact, the average level of IT security spend has remained flat over the last 3 years.

All while the dynamic and evolving nature of health IT increases the complexity of securing protected health information.

71% of respondents have widespread security concerns related to moving information and/or applications to the cloud, even though **3 of 4** providers are already using the cloud in some way.

95% of respondents identified more than one obstacle to securing medical devices.

Advancing a risk management program.

Healthcare organizations can take these steps to help advance their risk management program across their organization:

- **Create cybersecurity awareness** and increase training across the organization and as appropriate for the respective roles
- **Continue to engage the Board** on the implications and risks of underinvesting in cybersecurity resources and tools
- **Implement an integrated cyber defense platform** rather than deploying a collection of point products and solutions
- **Ensure all necessary stakeholders (IT, Legal, PR and Communications, Clinical Staff, Executives, etc.) are involved** in Incident Response planning

To learn more about the HIT Security and Risk Management research findings and building a resilient cyber defense strategy, visit **www.symantec.com/healthcare**.

Data from: HIMSS Analytics

Produced by: HIMSS Media www.himssmedia.com

References
1 HIMSS Analytics IT Security and Risk Management Study. Prepared for Symantec, December 20, 2017
2 Office for Civil Rights, U.S. Department of Health and Human Services. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf