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 Study1 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.

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

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 these reported breaches affected a total of 5,136,438 individuals.2

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.