

Operationalizing Healthcare Cybersecurity

Cybersecurity threats in the healthcare industry remain stronger than ever, and data breaches remain a top concern.

Healthcare organizations are trying to address increasing cybersecurity risks, but are their strategies working?



In November 2016 alone, 459,000 patient records were compromised¹

The second annual HIMSS Analytics HIT Security and Risk Management Study revealed progress healthcare organizations made in the last year as well as identified where there are still gaps:

Progress in 2016...

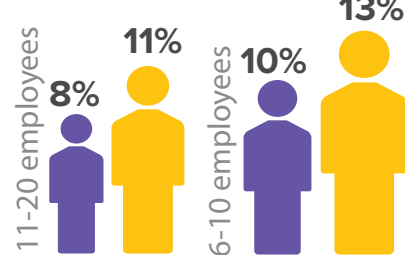
Cybersecurity budgets grew²:

Percentage of respondents who spend 7%-10% of their IT budget on cybersecurity jumped from 10% to 24% from 2015 to 2016



Distribution of employees allocated to IT security increased in 2016.³

2015
2016



More healthcare organizations are adopting established risk frameworks, with the NIST CSF most used by IT & security respondents.⁴



...But many healthcare organizations are still lagging

65% of participants are still spending less than 6% on security⁵:



Budget and staffing were ranked as the biggest barriers to higher levels of confidence in respondents' security programs⁶:



A significant number of respondents are in the early stages of addressing IT security for both medical and mobile devices, and some are still not addressing it at all.⁷

43%
Medical
27%
Mobile



Disparities create barriers

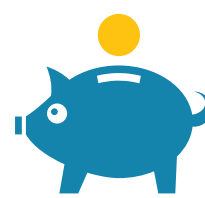
Disparities across clinical, business, security and IT stakeholders are further hindering the ability of organizations to advance their cyber posture:



Business leaders view cybersecurity as a business risk issue.



But clinical and IT leaders view it as a HIPAA compliance issue.⁸



To achieve a high level of cybersecurity confidence, business and IT leaders see a need for more investment in budgeting and staffing resources.



But clinical leaders say more employee awareness and training is needed.⁹

This disconnect impacts approaches to cybersecurity strategies.

All in for a Comprehensive Cybersecurity Strategy

While progress has been made over the past year, healthcare organizations still have a long way to go to fully protect their data and systems. The path to achieving success is much shorter when healthcare organizations follow these best practices:



Increase financial and human resources, but do so in a strategic manner.



Leverage a risk-based security framework to identify all cyber risks and resolve them more efficiently.



Develop and implement cybersecurity training across all departments.



Engage and empower all departments to participate in the operationalization of security practices.

To learn more about the HIT Security and Risk Management research findings and how your organization can operationalize cybersecurity, visit www.symantec.com/healthcare.