The path to health care insight:

EY 20th Global Information Security Survey 2017

Cybersecurity health sector results

EY
Building a better working world

Global findings

EY's 20th Global Information Security Survey (GISS) captures the responses of 1,105 C-suite leaders and information security and IT executives/managers, representing most of the world's largest and most-recognized global companies across 60 countries and nearly all industries. Of these, 37 respondents were from the health care industry.

The health sector continues to adjust security strategy and investment to match likely threats.

Health care organizations have increased their overall security functions since 2016, with more respondents reporting enhanced/strong capabilities. More companies report a lack of robust incidence response capability – this may be driven by better awareness of capability gaps.

The level of investment in information security has also increased from last year. Over three-quarters of companies plan to increase their information security budgets over the next 12 months. However, health care lags other industries in information security budget increases and there is wide-spread acceptance of the fact that further budget increases are required.

Health care respondents viewed budget constraints as the biggest obstacle or reason that challenges their information security operation's contribution and value to the organization. This may be due to boards' lack of knowledge about information security and suggests a need for clear articulation and messaging from the security team around alignment of information security initiatives with business needs, risk management and return on investment.

The need for higher investment and more effective security operations may be attributed to the increase in security incidents witnessed in health care since last year. Security incidents in health care remain higher than other industries. Total financial damages related to information security incidents has also increased. Though the increase in security incidents is true across industries, damages incurred in health care remain higher.

Download the full report at:
http://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2017-18

Key findings from the health sector

1. Health companies witness increase in security incidents

65% of respondents stated that they had a cybersecurity incident in the past 12 months (up 3% from last year).

57% of respondents from other industries stated that they had a cybersecurity incident in the past 12 months.

2. While most will increase the security budget this year, many think additional investment is needed

26% of respondents stated that their companies needed a 26%-50% increase in funding for cybersecurity.

10% of respondents want a 100% increase in funding for cybersecurity.

3. Cybersecurity spending slightly lags other industries

97% of respondents spend US$10m or less on cybersecurity annually (85% average across other sectors).

59% of respondents stated that their company's cybersecurity budgets increased over the past 12 months when compared to 63% in all other industries.

4. Security threat posed by external partners or vendors needs better management

49% more external partners submit self-assessment of security risk in health care than other industries (39%), which is less reliable.

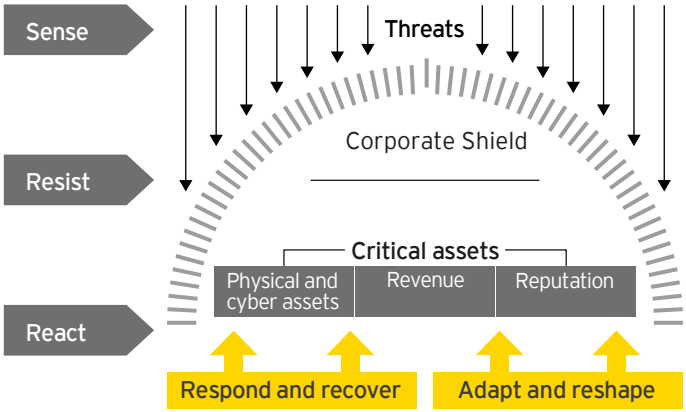
4% low implementation of maintaining an accurate inventory of third-party providers, network connections and data in health care vs. 46% overall.

5. Low cybersecurity awareness among board members

67% of respondents believe that their board does not have sufficient knowledge of information security.

83% of respondents stated that the person responsible for information security is not on the board.

Cyber-resilient health care



Today's cybersecurity landscape in health:

- Companies becoming more strategic and less reactionary in their cybersecurity spending
- Increasing consideration of security in the formulation of organizational and strategic plans
- More diligent in assessing external partners, vendors or contractors
- Low implementation of maintaining accurate inventory of third-party providers, network connections and data
- Criminals value customers' personal or identifiable health information
- Perceived risks and threats differ from high priority cybersecurity areas
- Perceived risk of Internet of Things (IoT) usage higher in health care; however, its adoption is hampered by budget constraints
- Information loss on a mobile device is of increasing concern

Key characteristics of a cyber-resilient health organization

Budgets without constraining effectiveness

Pressures on health companies' budgets have increased with the need to reduce costs and improve quality of care. Recognizing the strategic benefits of investment in information security is paramount. Including information security in the planning of overall strategy will aid health care companies in realizing savings from thwarted security incidents and resultant financial damages. This requires strategic budgeting for information security operations in line with the requirements of the organization.

Proactively defends against risks

Customers' personal or identifiable data is of high value to cyber criminals and has been increasingly targeted in attacks on health care companies. Ransomware attacks such as WannaCry exposed the vulnerabilities of health care organizations running outdated technology and crippled their day-to-day operations. This incident triggered a massive effort to reorganize and update cybersecurity measures in the National Health Service. By becoming less reactionary and more strategic in their response to cybersecurity incidents, health care companies can benefit as they proactively defend against their greatest risks and make them focus areas for building resilience.

Adopts technology with an understanding of risks involved

Applications of technologies such as IoT, blockchain and AI offer many advantages in terms of cost-cutting and efficiency improvement in health care. Any implementation of technology carries inherent security risks. Having in-depth, and preferably in-house, experience in the strategic planning of security measures and risk mitigation will aid health companies in utilizing these technologies with maximum efficiency.

Guards against internal and external risks

Health care companies are on average more diligent in assessing external partners, vendors or contractors. However, there is very low compliance with the practice of maintaining an accurate inventory of third-party providers, network connections and data. Guarding against all sources of information security risks, both internal and external, will elevate the cybersecurity resilience of health care organizations.

Promotes a cybersecurity-aware leadership

Awareness and understanding of cybersecurity risk, strategy and operations at the board level is essential to the overall functioning of a cyber-resilient health care company. Mandatory inclusion of information security representation on the boards of health care organizations will provide cybersecurity that is interwoven with the operations of the organization and not considered an afterthought.

To find out more about EY Global cybersecurity health offerings, please contact:

Liz Mann	+1 212 773 0437	liz.mann@ey.com
Rajesh Padiyal	+1 734 717 1501	rajesh.padiyal@ey.com
Laura B. Armstrong	+1 617 565 0541	laura.armstrong@ey.com

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EYG no. 00224-184GBL

BMC Agency

ED None.

ey.com/gl/en/industries/health