OnTrend

APRIL 2016 ISSUE

Cyber Security

Protecting critical health care information

OPTUM®

The trend

Cyber Security

As health care data security breaches proliferate, putting members' data at risk for fraud or identity theft and subjecting health plans to HIPAA fines and loss of reputation, health plans must address how they can strengthen information and network security to effectively protect health care information. Today, health care data breaches affect nearly one in three Americans, a statistic that can no longer be ignored.

Experts predict that cyberattacks on health care entities are likely to increase because they are lucrative; electronic health care information has 50 times the black market value of credit card data ($50 versus $1).[1] Importantly, health plans must upgrade security controls and monitoring activities so they are more mature, integrated and efficient, and broadly address cyber hackers.

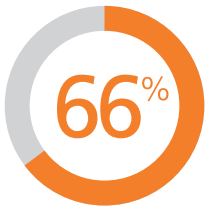
Why now?

From misplaced hard drives and stolen employee laptops to phishing and social engineering — cyberattackers take any opportunity to penetrate networks and steal confidential information. A national health plan that was hacked in 2015 has said that its breached data for 78 million people included Social Security numbers, income data, birthdates and other identifiers.[2] Such data are used to establish fraudulent accounts, can result in false insurance claims and may hinder the treatment of and the cost of care for members whose data are stolen.

200+ days

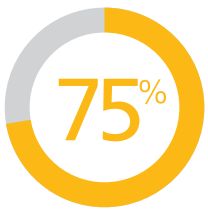
average time to **discover** a breach

Mandiant, A FireEye® Company. "M-Trends® 2015: A View from the Front Lines". Feb. 2015.



of payers consider themselves **ready to defend** against cyber attacks

Heller, Matthew. "Health Care's Cyber-Security Spend Found Lacking" CFO.com. Sept. 1, 2015.



of organizations are **unprepared** for cyber attack

Poneman, Larry. "The Cyber Resilient Organization: Learning to Thrive Against Threats". Ponemon Institute. Sept. 18, 2015.

Key statistics

- Health care represents **44 percent** of data breaches across all industries.[3]
- According to the Office for Civil Rights/ Department of Human Services, there have been 740 major health care breaches over the past five years.[4]
- Health care security breaches affect **one in three** Americans.[5]
- Health care organizations generally are not equipped to identify and stop data security breaches.[6]

Health care security breaches affect **one in three** Americans.

* DiChristopher, Tom. "Data breaches down in retail, but soaring in health care." CNBC. Dec. 24, 2015.

Impact on health plans

Increasingly severe and pervasive cyberattacks, along with emerging technologies that capitalize on vulnerabilities in data sharing and storage, pose a significant threat to health plans' business continuity.

It is imperative that health plans learn more about the gaps in their information and network security controls and employee behavior to mitigate financial penalties, such as $50,000 per HIPAA violation (or up to $1.5 million per year for identical, repeat violations), and damage to their organizations' reputation, with members filing an increasing number of lawsuits. Making cyber security a priority is a universal goal. In 2016, senior IT and business leaders say increasing priority is being placed on investments in information risk, compliance and security.[7]

Next steps

Health plans need to develop the appropriate security controls and implement continuous monitoring programs to remediate vulnerabilities and respond to the changing dynamic threat environment. A mature approach to security controls requires IT leaders to apply an outside-in lens to their operations, examining each layer — perimeter, networks, applications, databases, endpoints and users — along with physical assets like computers, tablets and mobile devices. For example, health plans should know whether their handling of protected health information (PHI) and personally identifiable information (PII) across each layer is sufficient to address current security risks and cyber threats.

Identifying risks and vulnerabilities and establishing an actionable road map are the first steps toward developing a mature security posture — one that provides the necessary security controls and ongoing monitoring to combat emerging threats and vulnerabilities across the organization.

Building an effective security organization

Learn more

optum.com/ontrend

1 Bitglass Healthcare Breach Report. 2014.

2 Leung, Lily. "O.C. Watchdog: Healthcare data breaches spike in California" Orange County Register. Jan. 15, 2016.

3 Id.

4 Abelson, Reed, and Goldstein, Matthew. "Anthem Hacking Points to Security Vulnerability of Health Care Industry." The New York Times. Feb. 6, 2015.

5 DiChristopher, Tom. "Data breaches down in retail, but soaring in health care." CNBC. Dec. 24, 2015.

6 Bitglass Healthcare Breach Report. 2014.

7 White, Andrew. "Information Risk, Security and Compliance Are Top Priorities in 2016." Gartner. Jan. 14, 2016.