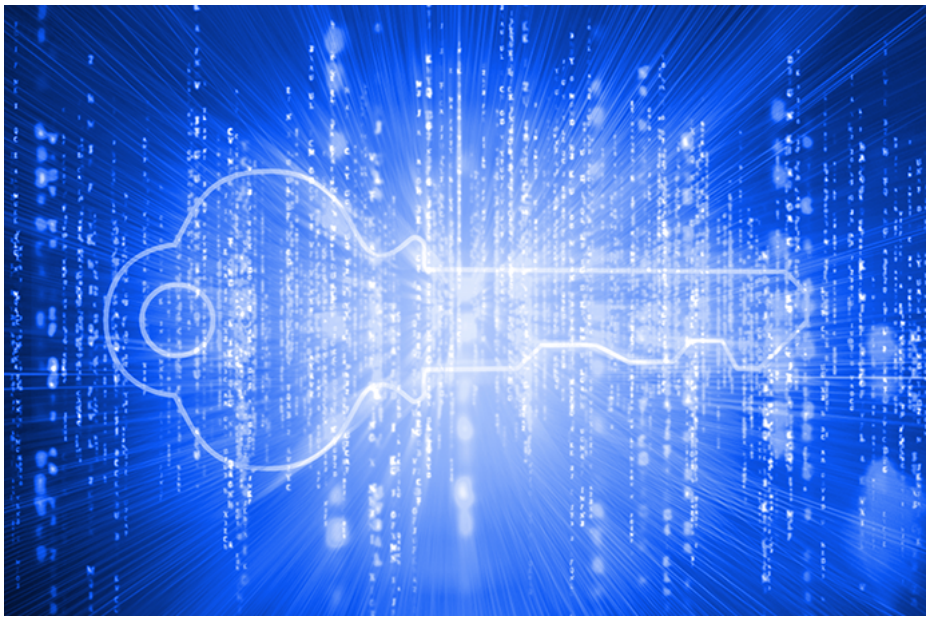
HIPAA Data Breaches, Cyber Attacks Reported by 47% of Orgs

KPMG found that there was a 10 percentage point increase in reported HIPAA data breaches or cyber attacks from 2015 to 2017.



Source: Thinkstock

By Elizabeth Snell (mailto:esnell@xtelligentmedia.com)

July 27, 2017 - There has been an increase over the past two years in healthcare providers and health plans experiencing HIPAA data breaches or cybersecurity attacks that compromised data, according to a recent KPMG survey.

The 2017 Cyber Healthcare & Life Sciences Survey found that 47 percent of providers and health plans said they had instances of security-related HIPAA violations or cybersecurity attacks impacting data. The **2015 KPMG survey (https://advisory.kpmg.us/content/dam/kpmg-advisory/PDFs/ManagementConsulting/2015/KPMG-2015-Cyber-Healthcare-Survey.pdf)** had 37 percent of respondents state the same.

However, 35 percent of respondents added that they are "completely ready" to defend against a concerted cyber attack, an increase from the 16 percent who reported such confidence in 2015.

For the survey, KPMG interviewed 100 respondents from healthcare providers and payers with over $500 million in annual revenue. Individuals held titles such as CIO, CTO, CSO or CISO.

KPMG Healthcare Advisory Leader Dion Sheidy said that healthcare payers and providers are on "treacherous ground" and that entities cannot underestimate cybersecurity risks.

READ MORE: Are Business Associates Unprepared in Health Data Protection? (https://healthitsecurity.com/news/are-business-associates-unprepared-in-health-data-protection)

"There needs to be a higher degree of vigilance among boards and executive suites as attacks become much more sophisticated, especially as doctors need to share information to improve quality and as connected medical devices and wearables proliferate," Sheidy explained in a statement. "The WannaCry ransomware hack in May was a warning shot against our collective ability to protect patient safety and privacy."

The report also found that even with increasing threats, there was a decrease in **cybersecurity being seen as a board agenda (https://healthitsecurity.com/news/how-cybersecurity-affects-the-evolving-healthcare-ciso-role)**. Seventy-nine percent of respondents said cybersecurity was a board topic, a decrease from the 87 percent reported in 2015.

There was also a smaller amount of information protection investments in the past 12 months, with 66 percent of respondents saying their organization had done so. The 2015 survey had 88 percent of those surveyed say their healthcare company invested in information protection in the previous year.

Sixty-three percent of respondents said data sharing with third parties was the biggest vulnerability. Other top vulnerabilities were Internet-enabled devices not being fully controlled by IT and having a lack of resources/budget.

Approximately one-third of total respondents – 32 percent – said that an attack vector resulted in **ransomware being introduced (https://healthitsecurity.com/features/how-ransomware-affects-hospital-data-security)** to their environment. Of those organizations affected by ransomware, 41 percent said they paid the ransom as an initial response. Twenty-five percent said they used a forensic cyber team to fix the problem, while 19 percent said they worked with authorities to pursue criminal action.

READ MORE: Cybersecurity Attacks Hit 87% of Organizations in 2016 (https://healthitsecurity.com/news/cybersecurity-attacks-hit-87-of-organizations-in-2016)

While some respondents did say investing in higher quality staffing was necessary to improve cybersecurity, more were opting to invest in technology.

Seventy-six percent of those surveyed said they planned to make greater investments in technology (i.e. software, firewalls, encryption), while 83 percent said they would invest in stronger policy/controls around data access and processes.

Forty-one percent of respondents said they planned to invest in hiring and training staff members and 44 percent reported to investing in governance.

Furthermore, 15 percent of respondents reported that increased or higher quality staffing was necessary to improve their organization's cybersecurity. Nearly one-quarter of those surveyed said an "overarching strategy" was the biggest need for improved cybersecurity.

"A solid cyber security program needs people, processes and technology and short-changing staff and the process structure needed to adequately govern, manage and monitor the technology is a faulty approach," said KPMG Cyber Security Group in Healthcare & Life Sciences Leader Michael Ebert. "Software can only protect you so far and staff is important when it comes time to respond to a data breach. The respondents that are not emphasizing staff and processes are underestimating the threats or creating a false sense of security among their management and board."

READ MORE: Healthcare Data Security Incidents Second Highest in 2016 (https://healthitsecurity.com/news/healthcare-data-security-incidents-second-highest-in-2016)

The KPMG report also found that government-sponsored hackers were the biggest cybersecurity threat among executives in charge of technology, information, and security at drug and medical device makers.

Fifty-three percent of respondents from pharmaceutical, biotech, and medical device organizations said government-sponsored attacks were the biggest threat, while 49 percent cited individual hackers, and 47 percent said "hacktivists" were the top threat.

Sixty-nine percent of respondents said financial information was the most likely targeted asset, followed by patents/clinical research (63 percent), competitive market analysis (49 percent), and employee personal identifiable information (45 percent). Just 30 percent of respondents believed that patient data was the asset that would most likely be targeted by bad actors.

A combination of technological investments and proper employee training was also cited by the **ISACA State of Cyber Security 2017 report (https://healthitsecurity.com/news/healthcare-cybersecurity-measures-must-evolve-for-success)** as necessary for healthcare cybersecurity success.

Training is necessary to address the cybersecurity skills gap, but one in four surveyed organizations said they have training budgets of less than US $1,000 per cybersecurity team member, the report found. Additionally, half of surveyed entities said they will see budget increases, down from 61 percent in 2016.

"Part of our report really flagged a glaring gap, given the acceleration of these type of attacks, the far-reaching area of these type of attacks," ISACA Board Director Rob Clyde told *HealthITSecurity.com* in a previous interview. "This is particularly true as we've seen it affecting the healthcare industry. On the flip side, our organizations aren't spending enough money to train and certify their security professionals."

Related Articles

- **Possible Health Data Breaches From Theft, Unauthorized Access (https://healthitsecurity.com/news/possible-health-data-breaches-from-theft-unauthorized-access)**
- **New Bill Hopes to Improve Health IT, Ease Regulations (https://healthitsecurity.com/news/new-bill-hopes-improve-health-ease-regulations)**
- **ONC, HIEs work on secure direct messaging during disasters (https://healthitsecurity.com/news/onc-hies-work-on-secure-messaging-during-disasters)**

Related Resources

- **Protecting Data in the Healthcare Industry (https://healthitsecurity.com/resources/white-papers/protecting-data-in-the-healthcare-industry)**
- **4 Critical Elements of a Successful GRC Implementation (https://healthitsecurity.com/resources/white-papers/4-critical-elements-of-a-successful-grc-implementation)**

• Navigating the Evolving Threat Landscape With a More Complete Approach to Network Security (https://healthitsecurity.com/resources/white-papers/navigating-the-evolving-threat-landscape-with-a-more-complete-approach-to-n)

Sign up to receive our newsletter and access our resources

Your email SUBMIT

Newsletter Signup

Join 50,000 of your peers and stay up to date on HIPAA, Ransomware, OCR Audits and IT Security.

- [x] Health IT Security (Twice Weekly)
- [ ] IT Infrastructure (Weekly)
- [ ] mHealth & Telehealth (Weekly)
- [ ] Interoperability (Weekly)
- [ ] Health Analytics (Twice Weekly)
- [ ] Revenue Cycle (Twice Weekly)

Your email

sign up

view our privacy policy (/privacy-policy)

Most Read Stories

HIPAA Data Breaches, Cyber Attacks Reported by 47% of Orgs (http://healthitsecurity.com/news/hipaa-data-breaches-cyber-attacks-reported-by-47-of-orgs)

Breaking Down HIPAA: Health Data Encryption Requirements (http://healthitsecurity.com/news/breaking-down-hipaa-health-data-encryption-requirements)

HHS Updates HIPAA Breach Reporting Tool, Empowers Consumers (http://healthitsecurity.com/news/hhs-updates-hipaa-breach-reporting-tool-empowers-consumers)

HIPAA Technical Safeguards: A Basic Review (http://healthitsecurity.com/news/hipaa-technical-safeguards-basic-review)

RevCycleIntelligence.com (https://revcycleintelligence.com)
mHealthIntelligence.com (https://mhealthintelligence.com)
HealthPayerIntelligence.com (https://healthpayerintelligence.com)
HITInfrastructure.com (https://hitinfrastructure.com)
PatientEngagementHIT.com (https://patientengagementhit.com)