Bitglass reports over 27 million affected by healthcare data breaches last year

SYDNEY – February 20 - Bitglass, the next-gen cloud security company, has released its sixth annual Healthcare Breach Report. Each year, Bitglass analyses data from the U.S. Department of Health and Human Services' 'Wall of Shame', a database containing information about breaches of protected health information (PHI). In 2019, these breaches collectively affected over 27 million individuals. Bitglass' latest report analyses the breaches of 2019, compares them to those of previous years, and reveals key trends and cybersecurity challenges facing the healthcare industry. Breaches recorded in the database are classified into the following categories: Hacking or IT incidents: Breaches related to malicious hackers and improper IT security Unauthorised access or disclosure: All unauthorised access and sharing of organisational data Loss or theft: Breaches enabled by the loss or theft of endpoint devices Other: Miscellaneous breaches and leaks related to items such as improper disposal of data According to the findings, the total number of records breached more than doubled from 2018 to 2019. This same doubling also occurred between 2017 and 2018, revealing a dramatic upward trend over the last few years. Corresponding with this, the average number of individuals affected per breach reached 71,311 in 2019, nearly twice that of 2018 (39,739). Additionally, this was the first time since 2016 that the number of breaches reached over 300--the 386 incidents in 2019 represented a 33% increase over 2018. "Last year, 'Hacking and IT incidents' was the top cause of breaches in healthcare, accounting for more than 60% of all data leakage," said Anurag Kahol, CTO of Bitglass. "This is not particularly surprising given the fact that threat actors are maturing their capabilities and adapting to security measures organizations put in place, like multi-factor authentication. "Healthcare databases are heavily targeted by cybercriminals as they hold a wealth of sensitive information like medical histories, Social Security numbers, personal financial data, and more. This means that healthcare firms must employ the appropriate technologies and cybersecurity best practices to ensure all data within their IT systems is secure around the clocks." Key findings The cost per breached record in healthcare was $429 in 2019. Last year, with 27.5 million records exposed, data breaches cost healthcare organisations $11.8 billion. Around 24 million people were affected by healthcare breaches due to hacking and IT incidents. This category was followed by unauthorised access or disclosure, which affected 2.5 million people. Lost or Stolen Devices has consistently had the biggest annual decrease over the past few years, dropping from 148 in 2014 to 42 in 2019. The total number of records breached has more than doubled each year; from 4.7M in 2017 to 11.5M in 2018, and to 27.5M in 2019. To learn more about the state of cybersecurity within the healthcare industry over the past year, download the full report here: https://pages.bitglass.com/CD-FY20Q1---2020-Healthcare-Breach-Report_LP.html?&utm_source=pr About Bitglass Bitglass, the Next-Gen Cloud Security company, is based in Silicon Valley with offices worldwide. The company's cloud security solutions deliver zero-day, agentless, data and threat protection for any app, any device, anywhere. Bitglass is backed by Tier 1 investors and was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution. ANZ media contact David Frost TouchdownPR for Bitglass 02 7902 9567

Contacts

David Frost
(02) 7903 9567
mailto: davidf@prdeadlines.com.au