http://www.telecomkh.com/en/internet/news/9128
Healthcare breaches reach high in 2016, drop-off in early 2017
09/06/16

Date: ***Fri, 06/09/2017 - 12:08*** Source: Bitglass

Despite historic volume of breaches, overall number of compromised records declines year-over-year

Eduard Meelhuysen, VP Sales EMEA, BitGlass, at NetEvents European Media Spotlight "Innnovators in cloud, IoT, IA & Security", London

PHOTO / telecomkh.com

Bitglass, the Total Data Protection company, announced that in 2016 healthcare breaches hit an all-time high (328), surpassing the previous record set in 2015 (268). Records of approximately 16.6 million Americans were exposed as a result of hacks, lost or stolen devices, unauthorized disclosure and more. Good news, however, is that the overall number of compromised records has declined for the second year in a row and early indications suggest that those numbers will continue to decline in 2017. These and other statistics are contained in the Bitglass 2017 Healthcare Breach Report.
The third annual Healthcare Breach Report aggregates data from the U.S. Department of Health and Human Services' Wall of Shame – a database of breach disclosures required as part of the Health Insurance Portability and Accountability Act (HIPAA) – to identify the most common causes of data leakage. Bitglass explored the changes in breach frequency as well as the preventative steps organizations have taken to limit the impact of each breach in 2016 and in the first quarter of 2017.

The key Bitglass report findings include:
• Breaches hit all-time high – 328 U.S. healthcare firms reported data breaches in 2016, up

from 268 in 2015.
• Volume of leaked records falls in 2016, on track to fall further in 2017 – 16.6 million Americans were affected by breaches throughout 2016, down significantly from 2015 even when excluding
the massive Anthem breach.
• Unauthorized disclosures now the leading cause of breaches – accounted for nearly 40 percent
of breaches in 2016.
• Hacking and IT incidents continue to pose the greatest risk – the volume of records that leak
because of hacking is greater than all other breach events combined.
• All five of the largest breaches were the result of hacking and IT incidents in 2016 - to put that in perspective, 80 percent of leaked records in 2016 were the result of hacking. So far in 2017, the largest breach was the result of theft and the four next largest breaches
were due to hacking.

“Breaches and information leaks are unavoidable in every industry, but healthcare remains one of the biggest targets,” said Nat Kausik, CEO, Bitglass. “While threats to sensitive healthcare data will persist, increased investments in data-centric security and stronger compliance and disclosure mandates are driving down the impact of each breach events.”

Breach Costs Hit Record High
According to data from the Ponemon Institute, the average breach costs U.S. companies is $221 per lost record, which is up from $217 per record in 2015. The cost per leaked record for healthcare firms topped $402 in 2016 – which is a massive cost given the number of records lost because hacking-related breaches. Given the significant value of healthcare data – Social Security numbers, treatment records, credit information and more sensitive personal information – the cost of a breach to a hospital or health system can be devastating.

Why Healthcare Data?
Unlike credit card breaches, where limited liability laws offer some protection, victims have little recourse when subject to identity theft via PHI leaks. Identity theft is not the sole use for this highly sensitive data – criminals can access medical care in the victim’s name or even conduct corporate extortion using PHI. Under HIPAA, organizations dealing with PHI must implement several technical safeguards. Find details on how CASBs can help you achieve compliance and protect against cloud data breaches in the full 2017 Healthcare Breach report.