




Healthcare Breach Report 2018

Security Procedures Thwart Attacks

 bitglass

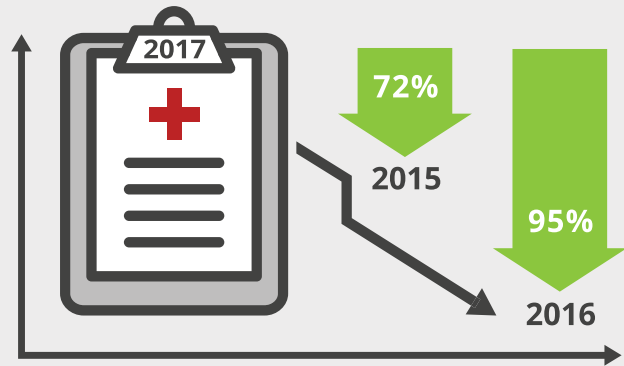
The background of the image consists of several shelves filled with numerous file folders. The folders are organized into rows and columns, with their colorful tabs (blue, red, green, yellow) visible. The perspective is from a slightly elevated angle, looking down at the shelves. The lighting is bright, highlighting the texture of the paper and the density of the folders.

Health data is among the most sensitive categories of information because it contains everything from your medical history to your social security number, possibly even credit card data. Naturally, acquiring this data is top of mind for hackers across the globe. Bitglass has carefully tracked and analyzed the state of data security in the healthcare sector since the beginning of 2014.

In 2017, as with prior years, hackers successfully made off with millions of individuals' protected health information (PHI). Health organizations, however, have made great strides in mitigating threats to PHI and in 2017, greatly reduced the total number of medical records breached.

Bitglass' fourth-annual Healthcare Breach Report analyzes data from the US Department of Health and Human Services' "Wall of Shame," where organizations that store or handle PHI are required to disclose breaches that affect at least 500 individuals. Read on to learn more about the breaches that caused the most damage in 2017 and to look at the year ahead in data security.

KEY FINDINGS



The number of breached healthcare records decreased by 72% since 2015 and 95% since 2016.

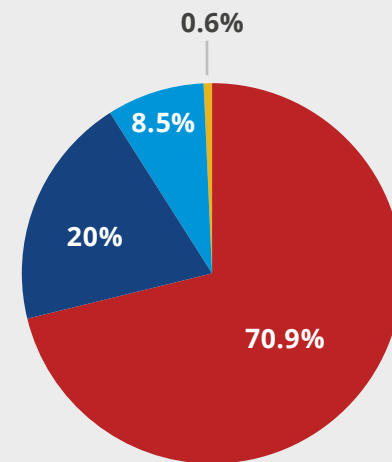


The number of hacking and IT Incidents have increased, but organizations have done a better job mitigating damage, with 16060 records compromised on average in 2017.



Over the past four years, healthcare organizations have consistently reduced the number of incidents attributed to lost and stolen devices.

2017 Breaches

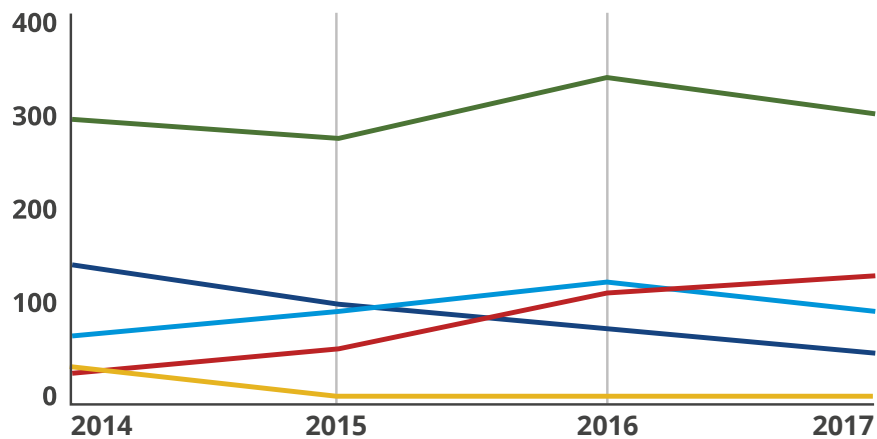


● Hacking/IT Incident ● Loss/Theft ● Unauthorized Disclosure ● Other

IT incidents on the rise

While the number of breaches remains steady at 294, down slightly from 2016 (328), healthcare remains a significant target for hackers. Specifically, the number of breaches due to hacking and IT incidents comprised nearly 71 percent, more than any other breach cause, and a trend that has steadily increased year-on-year since Bitglass began tracking this back in 2014.

Breach Count



● Hacking/IT Incident ● Loss/Theft ● Unauthorized Disclosure ● Other ● Total

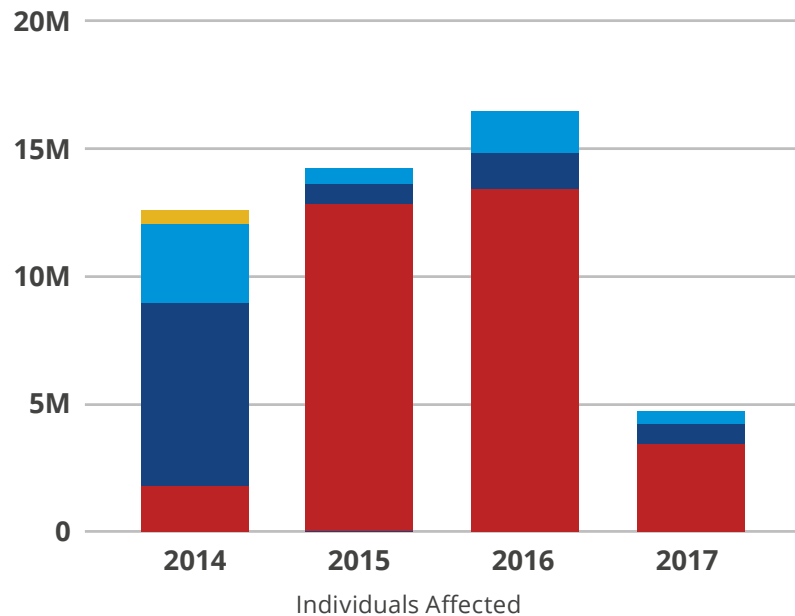


Number of individuals affected at a four year low

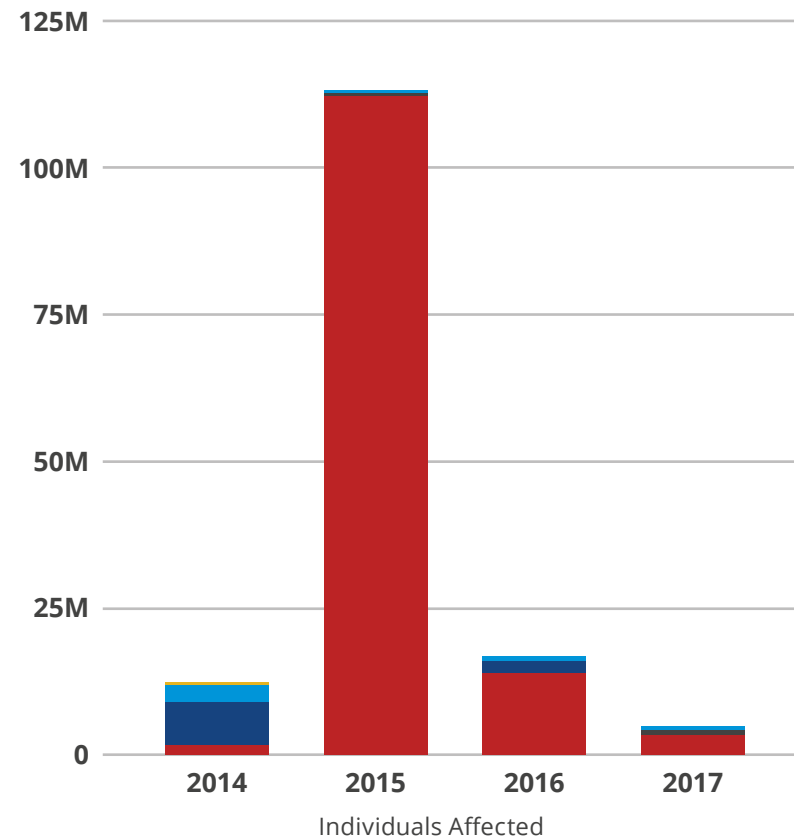
Even if we exclude the Anthem and Premera Blue Cross megabreaches of 2015, last year was the lowest in some time in terms of the overall impact of each attack. Organizations have put mechanisms in place to limit the number of lost

records and individuals affected. Whether it's rapid detection through behavior analytics, proactive security like encryption and redaction, or a combination of security practices, all are effective means of mitigating breach risk.

Individuals Affected
Excluding Megabreaches



Individuals Affected
Including Megabreaches



● Hacking/IT Incident ● Loss/Theft ● Unauthorized Disclosure ● Other

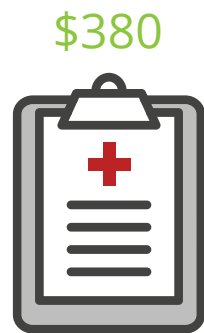
Breach costs 2018

According to data from the [Ponemon Institute](#), the cost per leaked record in the healthcare sector has once again risen, from \$369 in 2016 to \$380 in 2017. For an organization subject to a large-scale IT incident, that can represent hundreds of millions in cost for identity theft protection, IT forensics, and government fines.

Cost per Leaked Record



2016



2017



How One Healthcare Organization is Mitigating Cloud Risks

John Muir Health is one example of a major healthcare firm with over 6000 employees and more than 1000 affiliated, “community physicians.” Like most healthcare organizations, John Muir must balance demands to adopt cloud and BYOD with the need to protect PHI.

While Office 365, unmanaged device access, and external sharing provide increased productivity and mobility, they can also increase the risk of data leakage. Having adopted popular cloud apps like Office 365, the same features that provide increased productivity and mobility, including unmanaged device access and external sharing, can also increase the risk of data leakage.

As it migrates to cloud, John Muir leverages Bitglass’ CASB to mitigate the top three causes of breaches. Examples of key enabling features include:

Hacking/IT Incidents—credential hijacking and account compromise control; real-time incident discovery and management.

Loss/Theft—real-time control over PHI access; agentless mobile data protection without MDM

Unauthorized Disclosure—access control for any cloud application; external sharing controls.



Appendix

Individuals Affected	2014	2015	2016	2017
Hacking/IT Incident	1,677,469	111,812,172*	13,426,813	3,348,321
Loss/Theft	7,380,580	798,829	1,462,403	946,037
Unauthorized Disclosure	3,027,697	573,752	1,641,006	399,893
Other	477,041	82,421	125,730	27,593
Total	12,562,787	113,267,174	16,655,952	4,721,844

**includes outlier mega-breaches that collectively affected nearly 100M individuals*

Breach Count	2014	2015	2016	2017
Hacking/IT Incident	30	57	113	132
Loss/Theft	148	104	78	55
Unauthorized Disclosure	75	101	130	99
Other	36	6	7	8
Total	289	268	328	294

About Bitglass

Bitglass' Total Cloud Security Platform is the only secure access service edge offering that combines a Gartner-MQ-Leading cloud access security broker, the world's only on-device secure web gateway, and zero trust network access to secure any interaction. Its Polyscale Architecture boasts an industry-leading uptime of 99.99% and delivers unrivaled performance and real-time scalability to any location in the world. Based in Silicon Valley with offices worldwide, the company 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.

For more information, visit
www.bitglass.com



(408) 337-0190 | info@bitglass.com