# Healthcare Breach Report 2016

## WHAT A DIFFERENCE A YEAR MAKES

BITGLASS REPORT

bitglass

Primary source of data breaches:

**68%**

**lost or stolen employee devices**

2014

**98%**

**large scale data hacks**

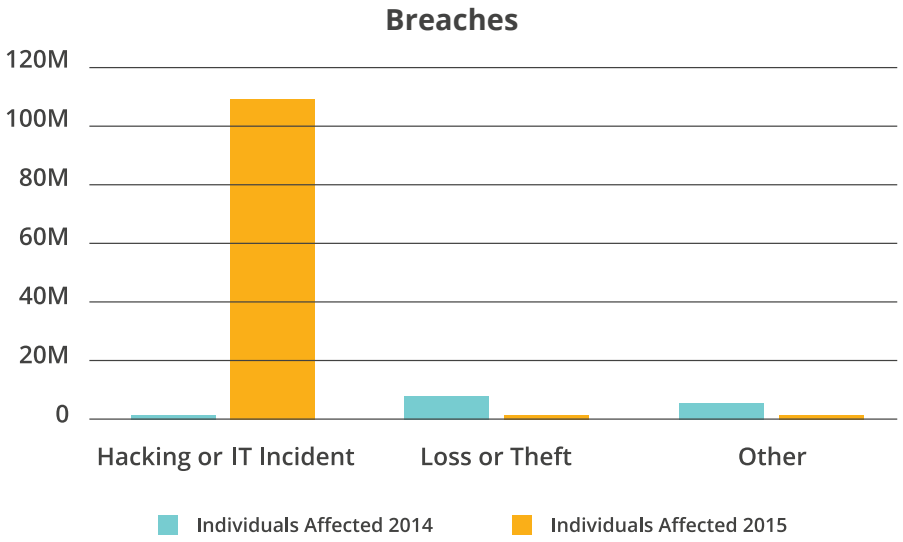
2015

In our last healthcare breach report, we identified loss and theft of employee devices as the primary source of breaches. In 2015, however, hacking and IT-related incidents resulted in 98% of leaked records, due in large part to a series of large-scale hacks that each affected over 10M individuals. These breaches include the widely publicized Premera Blue Cross hack involving 11M customers and the Anthem hack that resulted in 78.8M leaked customer records. Even if we were to exclude the 6 breaches that affected over 1M individuals, hacking and IT-related incidents would still account for a majority of leaked records.

In this report, we will explain why hackers are targeting this data, detail the techniques used by hackers, and identify ways that healthcare organizations can secure data and limit the risk of future breaches.

HIPAA regulations require that health organizations disclose all breaches that affect more than 500 people. This data, published by the US Department of Health and Human Services on their "Wall of Shame", reveals the shift toward hacking as the primary threat to healthcare data.

- In 2015, over 111M individuals' data was lost due to hacking or IT incidents in the US alone.
- There have been 56 breaches due to hacking or IT incidents in 2015, up from 31 in 2014.
- Only 97 breaches were due to loss or theft last year, down from 140 in 2014.
- Bitglass' latest **Cloud Adoption report** reveals 37% of organizations within the healthcare industry use Google Apps or Office 365, up from 8% in 2014, but only 5.2% of healthcare organizations are using Single Sign-on, the most basic security precaution, with these apps.




**One in three Americans were affected by healthcare breaches in 2015.** The following sensitive personal data has leaked in the past year:

- Name
- Address
- Date of Birth
- Social Security number
- Medical claims information

| Type of Breach | Individuals Affected **2014** | Individuals Affected **2015** |
|---|---|---|
| Hacking or IT Incident | 1,786,630 | 111,803,342 |
| Loss or Theft | 7,273,157 | 750,802 |
| Other | 3,504,350 | 646,243 |
| Total Individuals Affected | **12,564,137** | **113,200,387** |


# Why are hackers targeting healthcare data?

Protected health information, which includes such sensitive information as Social Security numbers, medical record numbers, date of birth, and more, is an incredibly valuable commodity on the black market. A recent Ponemon Institute report on the cost of breaches revealed the average cost per lost or stolen record to be $154. That number skyrockets to $363 on average for healthcare organizations.

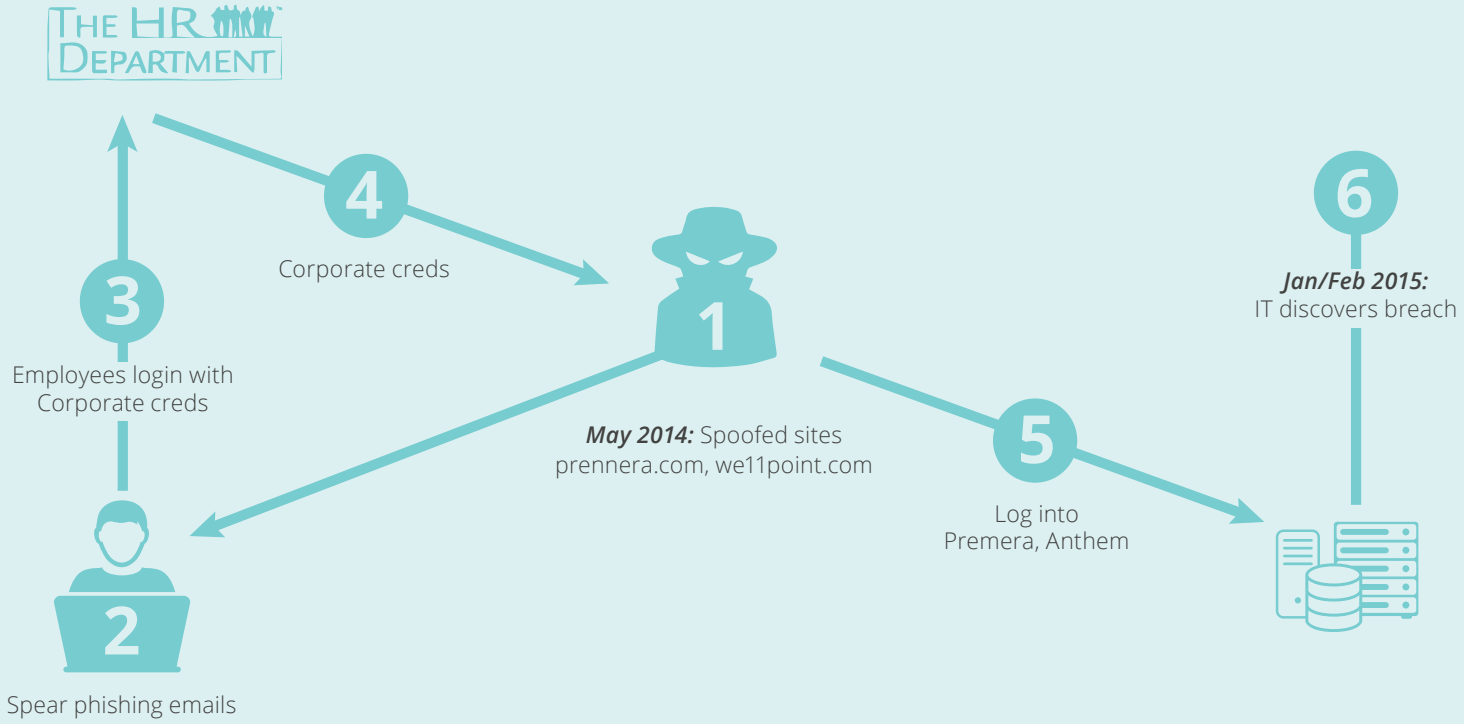
Unlike a credit card, where the issuer can simply halt all transactions and laws exist to limit an individual's liability, few are promptly informed of PHI leaks and have little recourse when subject to identity theft and the costs can be incredibly high. Your credit could be negatively affected, there is risk of financial loss, and while requesting a new credit card number is easy, changing a Social Security number is a cumbersome, drawn-out process.

While often used for the purposes of identity theft, criminals can use healthcare data for access to medical care in the victim's name or corporate extortion. Earlier this year, the Wall Street Journal reported on several fraudulent medical care cases, among them a worker who received a bill for a leg-injury treatment and a retiree mistakenly charged for a surgical operation. These many malicious use-cases underscore the importance of securing sensitive healthcare data.

# What happened in the Anthem and Premera breaches?

Results of an investigation reveal that at least one administrator's credentials were compromised in the Anthem breach and that the company's healthcare data was targeted by hackers in China. Access to these credentials provided the hackers with access to customer names, dates of birth, Social Security numbers, healthcare ID numbers, income data, and more. In the case of Premera, bank account and medical claims information were also potentially leaked.

It is believed that these credentials were stolen by means of a phishing attack where hackers used a technique called domain spoofing.




Hackers registered variations on the real domains, "prennera.com" in the case of Premera and "we11point.com" in the case of the Anthem breach

Phishing emails were sent to employees to bait them onto the spoofed sites

Employees log into the fake site with their credentials, giving hackers the credentials

Employees are then logged into the real Premera or Anthem site, unaware of the fact that they have just been subject to a phishing attack

# Protecting against major breaches

Under HIPAA, organizations dealing with protected health information must implement several technical safeguards: control over access, audit, data integrity, user authentication, and transmission security. A cloud access security broker (CASB) can provide healthcare organizations with the capabilities necessary to protect data in the cloud and achieve compliance.

**Control Access—**With a CASB, healthcare organizations can manage access to PHI stored in public cloud apps across both managed and unmanaged devices. CASBs offer robust DLP and DRM capabilities such that IT administrators can set policies to limit access by role or region, useful in the case of Anthem, where compromised credentials were used in an unusual location—China.

**Secure BYOD—**As demand for BYOD in healthcare rises, organizations need a means of protecting sensitive data on employee devices without impeding user privacy. There is a clear need for an agentless solution that allows healthcare organizations to remain compliant under HIPAA with control over data as it flows to the device and once on the end-user's device.

**Visibility—**To comply with HIPAA's audit requirement, IT can use a CASB for deep visibility into user activities with logs on how data is being shared and which users are accessing that data.

**Integrated Identity Management—**With an integrated identity solution, organizations can both maintain control over the key access point to their data and easily manage user account credentials. In addition, SSO, multi-factor authentication, and the like provide a more secure means of authenticating users and help minimize risk of breaches due to stolen credentials.

In light of the major breaches across 2015, securing healthcare data has never been more critical. The cost of losing each customer record is incredibly high and as hackers become more sophisticated, healthcare organizations need a HIPAA-compliant, comprehensive, data-centric solution. Fortunately, CASB technology provides organizations complete control over PHI, deep visibility, a means of securely authenticating users, and agentless mobile security.

bitglass

## 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**

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