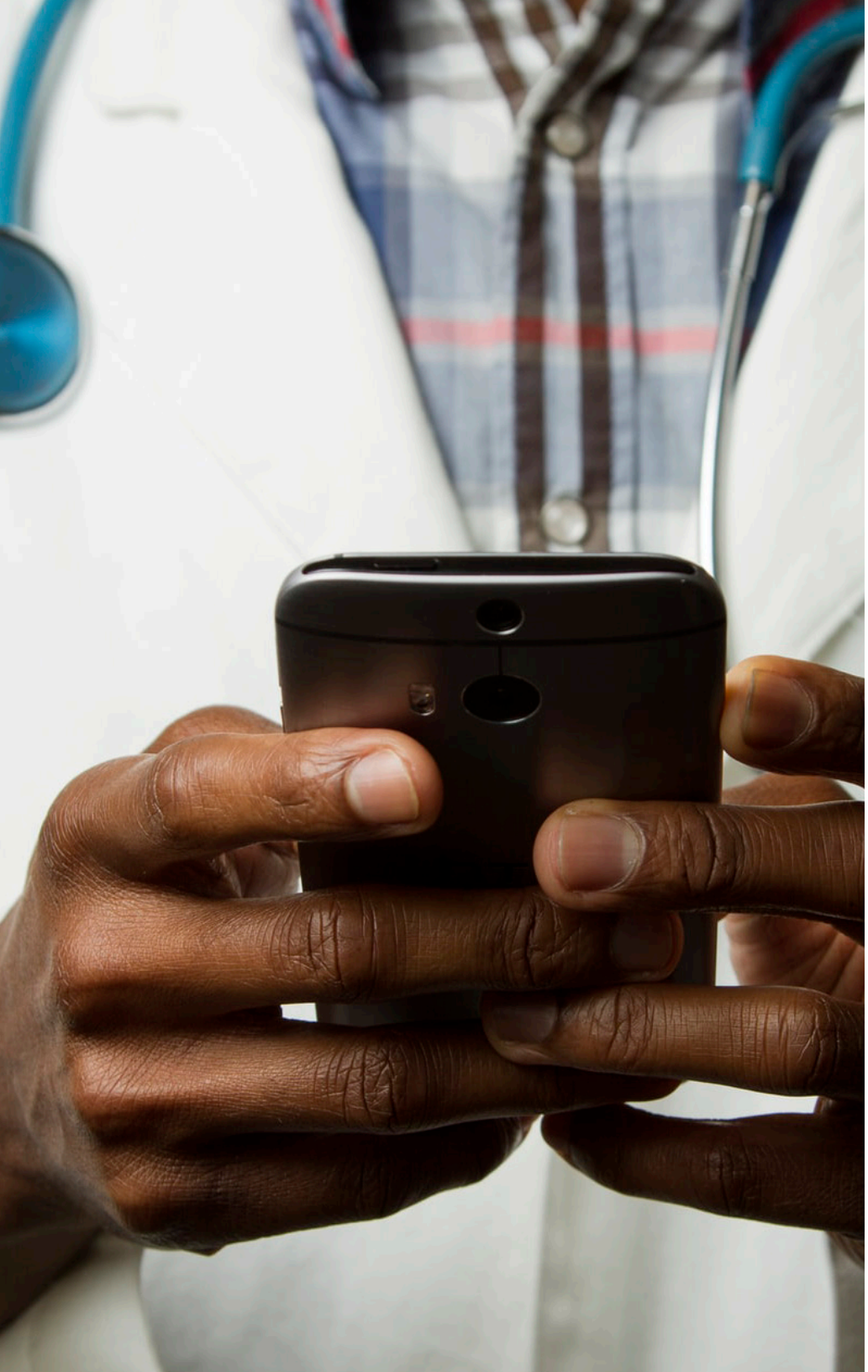
bitglass

Healthcare Breach Report 2020

Breaches on the Upsurge



The vast majority of healthcare organizations process and store protected health information (PHI), which is composed of sensitive patient data like medical histories, Social Security numbers, personal financial data, and more. Undoubtedly, this sensitive information attracts a great deal of attention from malicious entities that aim to exploit it for monetary gain.

In this sixth annual Healthcare Breach Report, Bitglass analyzes data from the U.S. Department of Health and Human Services' "Wall of Shame." The database includes PHI from breaches that collectively affected over 27 million individuals. These breaches are broken into the following categories:

Hacking and IT Incidents: Breaches related to malicious hackers and improper IT security.

Unauthorized Access or Disclosure: All unauthorized access and sharing of PHI.

Loss or Theft: Breaches enabled by the loss or theft of endpoint devices.

Other: Miscellaneous breaches and leaks related to items like improper disposal of data.

By analyzing this data, Bitglass uncovered the state of security for healthcare organizations in 2019.

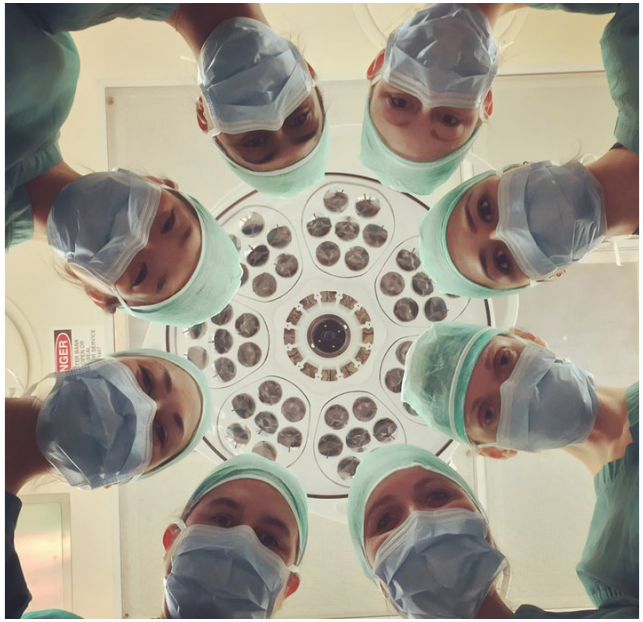
Key Findings

Despite the decreasing number of breaches per year, the count of healthcare breaches reached 386 in 2019, a 33% increase since 2018 (290).

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.

Hacking and IT Incidents (60.6%) was the top breach cause in healthcare in 2019, a dramatic increase from 45.8% in 2018.

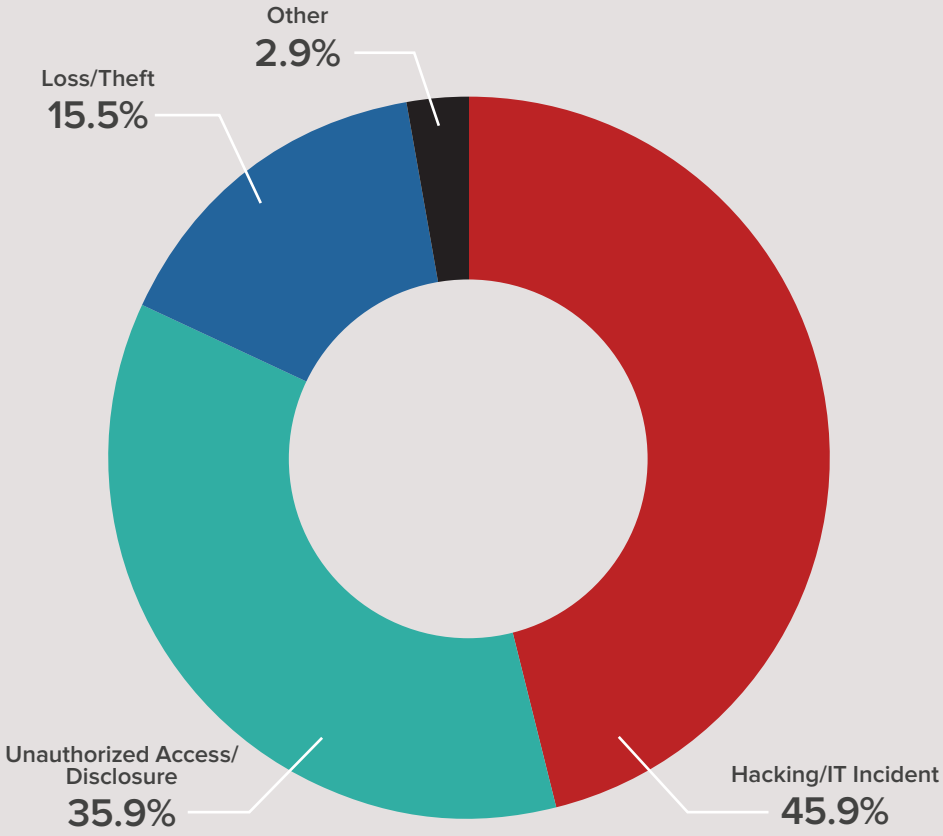
The average number of individuals affected per breach reached 71,311 in 2019, nearly twice that of 2018 (39,739).



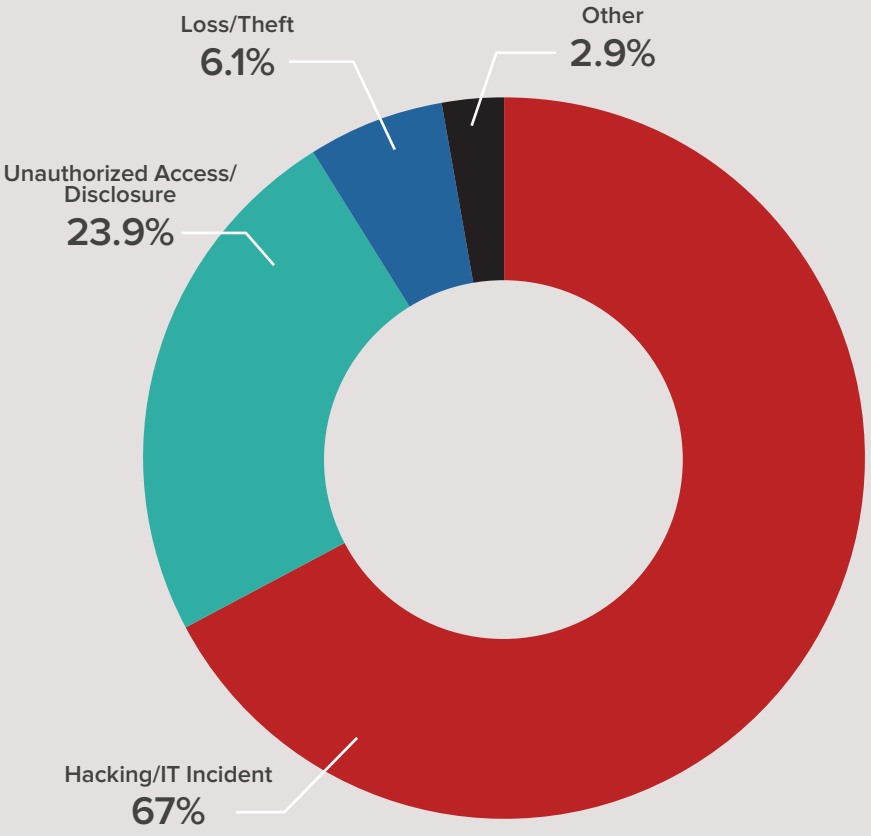
Lost and stolen devices lead to fewer and fewer breaches each year, dropping from 148 in 2014 to 42 in 2019.

2019 at a Glance

Breach Causes

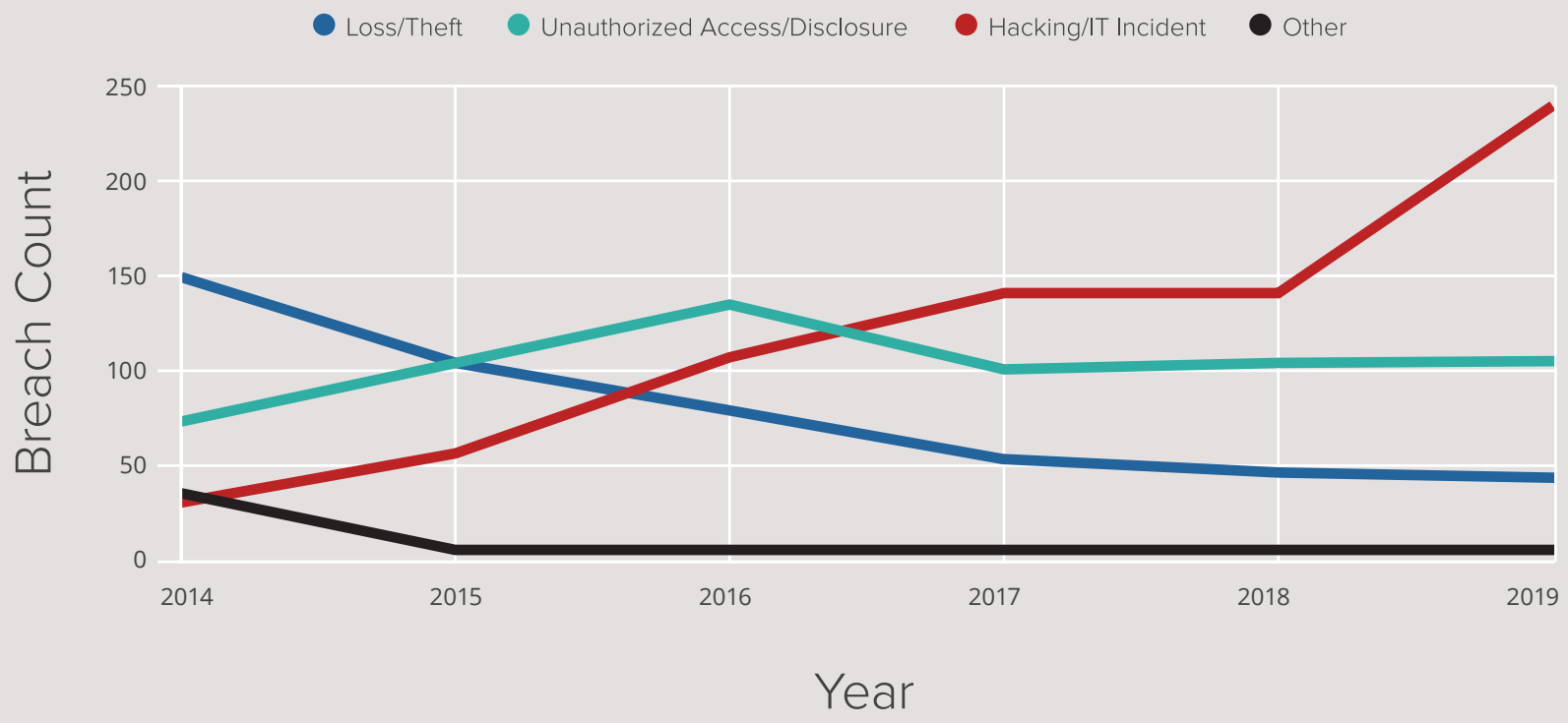


Individuals Affected



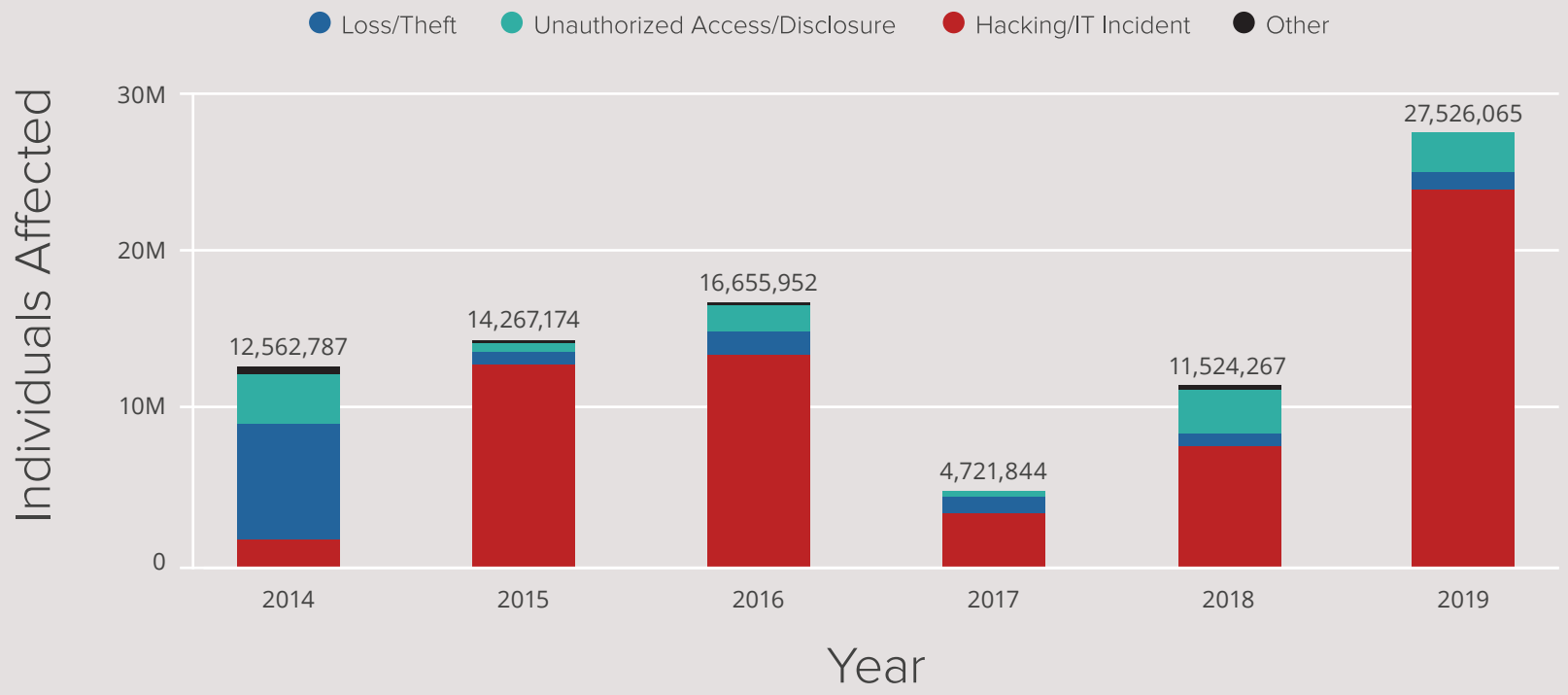
In 2019, Hacking and IT Incidents led to 60.6% of healthcare breaches. Relative to other breach causes, this category impacted a disproportionate percentage of individuals (86.7%), meaning that these leaks were larger on average. Nearly 24 million persons affected by healthcare breaches had their information exposed by Hacking and IT Incidents, while all other categories combined affected 3.6 million. This means that failing to protect data in IT environments can enable breaches of particularly large scales.

Breach Causes Year Over Year



While lost and stolen devices may have been the primary reasons for breaches in 2014, the prevailing threat today is Hacking and IT Incidents. This category, which has been growing in impact every year, increased exponentially in 2019. As organizations continue to embrace cloud migration and digital transformation, this trend will likely continue. As such, healthcare organizations must leverage the proper tools to successfully protect patient records and respond to the growing volume of threats to their IT ecosystems.

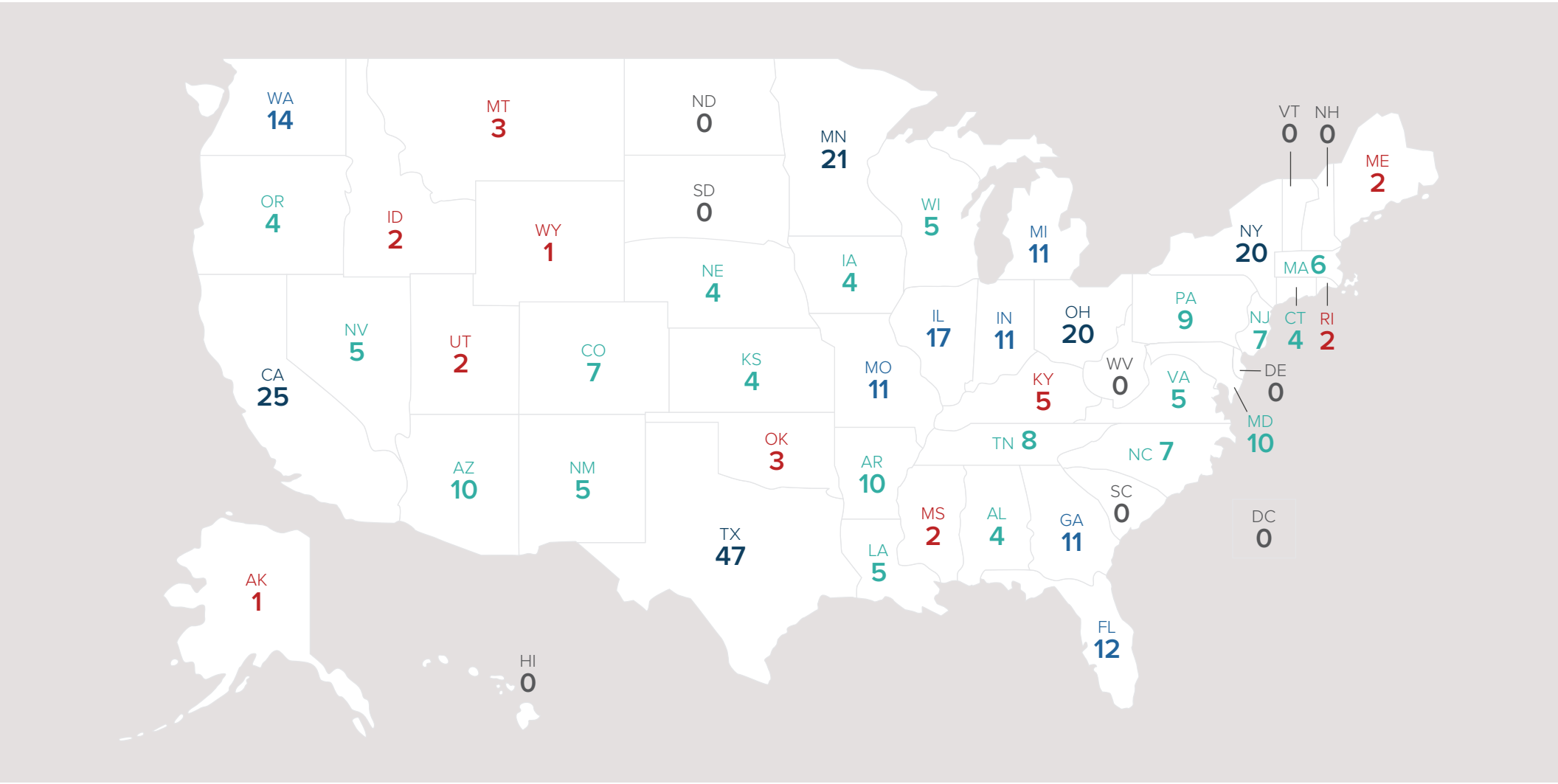
Individuals Affected Year Over Year



In addition to the overwhelming increase in the number of healthcare breaches in 2019, the number of individuals affected by said breaches was nearly twice that of 2018. As displayed in the chart above, this growth in breach frequency and size was fueled by Hacking and IT Incidents. Additionally, this chart includes the Douglas County Hospital DBA Alomere Health breach from 2019, which affected 10,251,784 individuals. 2019 also saw 15 separate breaches that affected facilities connected to Texas Health Resources which collectively compromised the data of 369,614 patients. The average number of individuals affected per breach in 2019 was 71,311, nearly twice that of last year.

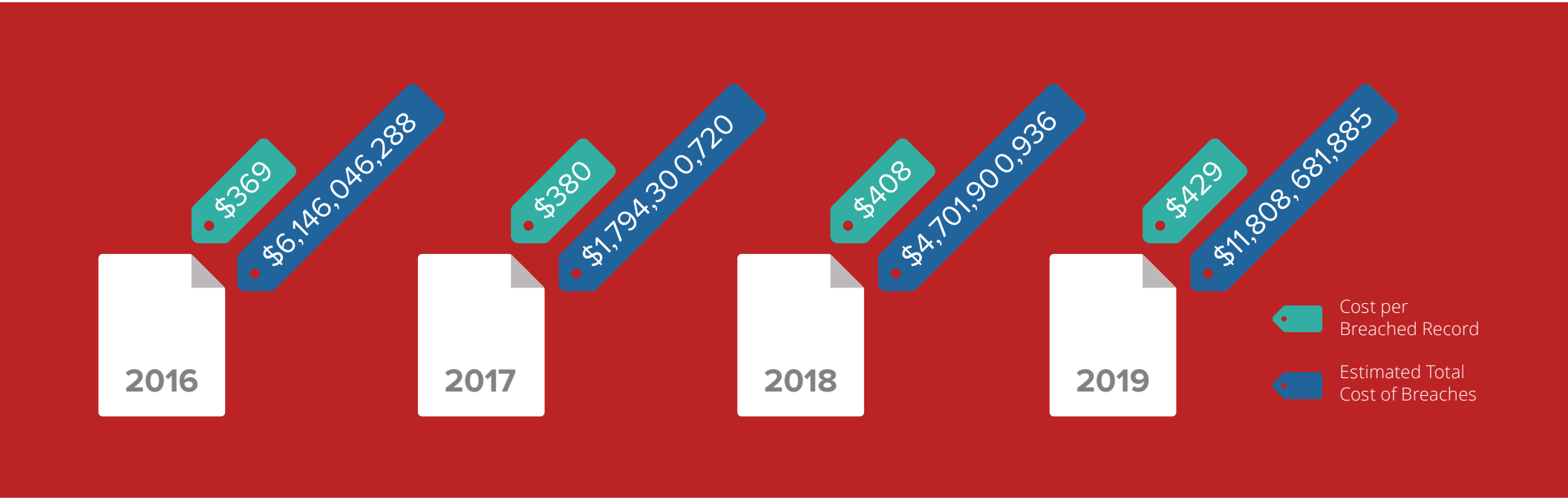
At 23,862,875, Hacking and IT incidents affected more individuals than any other breach cause in 2019 (as they have each year since 2015).

Breaches by State



Undoubtedly Texas (47) had the most healthcare breaches in 2019, nearly double the amount of California (25). This year, Texas experienced far more breaches than any other state in the past, an alarming feat considering the fact that California's state population outweighs Texas by 10 million. This is primarily due to the aforementioned chain of breaches associated with Texas Health Resources; 15 organizations were affected in October 2019.

The Cost of a Breach in 2019



According to data from the Ponemon Institute, the cost per record for a healthcare breach amounted to $429 in 2019. This is the highest per-record cost of any industry—finance ($210) comes in second and government ($78) lands last. Additionally, $429 represents a 3.5% increase over 2018 and a 11.4% increase since 2017.

Compounding the above problem is the fact that healthcare firms took a mean time of 236 days to identify breaches (the longest for any industry) and a mean time of 93 days to contain them (also the longest for any industry).

By combining the cost per breached record and the total number of records exposed, the overall cost of healthcare breaches for each year can be calculated. As shown here, billions of dollars are wasted annually because of improper cybersecurity in healthcare. As can be seen below, the number of breaches, as well as the overall cost in 2019 more than doubled since 2018.

Appendix

Breach Count	2014	2015*	2016	2017	2018	2019
Hacking/IT Incident	30	57	113	132	133	234
Loss/Theft	148	104	78	55	45	42
Unauthorized Access/ Disclosure	75	101	130	99	104	106
Other	36	6	7	8	8	4
Total	**289**	**268**	**328**	**294**	**290**	**386**

Individuals Affected	2014	2015*	2016	2017	2018	2019
Hacking/IT Incident	1,677,469	12,812,172	13,426,813	3,348,321	7,719,964	23,862,875
Loss/Theft	7,380,580	798,829	1,462,403	946,037	705,528	1,108,123
Unauthorized Access/Disclosure	3,027,697	573,752	1,641,006	399,893	2,760,037	2,542,390
Other	477,041	82,421	125,730	27,593	338,738	12,677
Total	**12,562,787**	**14,267,174**	**16,655,952**	**4,721,844**	**11,524,267**	**27,526,065**

*Excludes outlier mega-breaches for 2015 that affected approximately 90M individuals

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.

For more information, visit **www.bitglass.com**

bitglass

(408) 337-0190
info@bitglass.com