Healthcare Breach Report 2019

Hacking and IT Incidents on the Rise

bitglass

Healthcare organizations regularly handle protected health information (PHI), one of the most sensitive categories of data. Regulated under HIPAA, PHI encompasses medical history, Social Security numbers, personal financial data, and much more. Naturally, this data constitutes an attractive target for malicious parties looking to appropriate private information for profit.

Bitglass' fifth annual Healthcare Breach Report analyzes the data from the US Department of Health and Human Services' "Wall of Shame." The database contains information about breaches of PHI that affected more than 500 individuals. Each recorded breach belongs to one of the four categories below.

- **Hacking or 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 parsing the data, Bitglass uncovered the state of security for healthcare organizations in 2018.

Key Findings

Since 2016, the number of reported breaches has decreased each year; 2018's 290 represents a three-year low.

The total number of records breached more than doubled from 2017 to 2018—from 4.7M to 11.5M. Both years saw fewer records exposed than the prior three years (2014, 2015, and 2016).
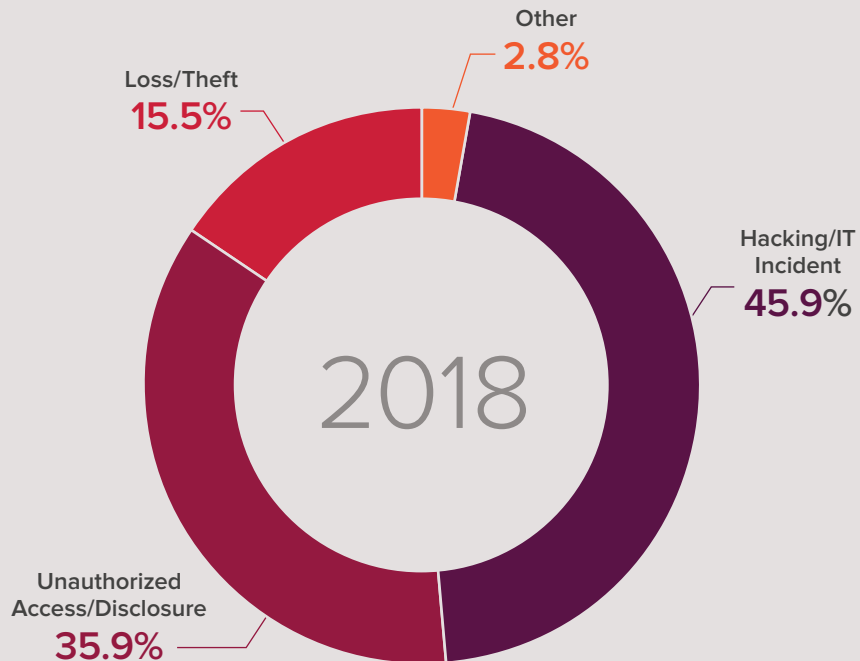
Hacking and IT incidents (45.9%) and unauthorized access and disclosure (35.9%) were the top breach causes in healthcare in 2018.

The average number of individuals affected per breach reached 39,739 in 2018, more than twice that of 2017 (16,060).
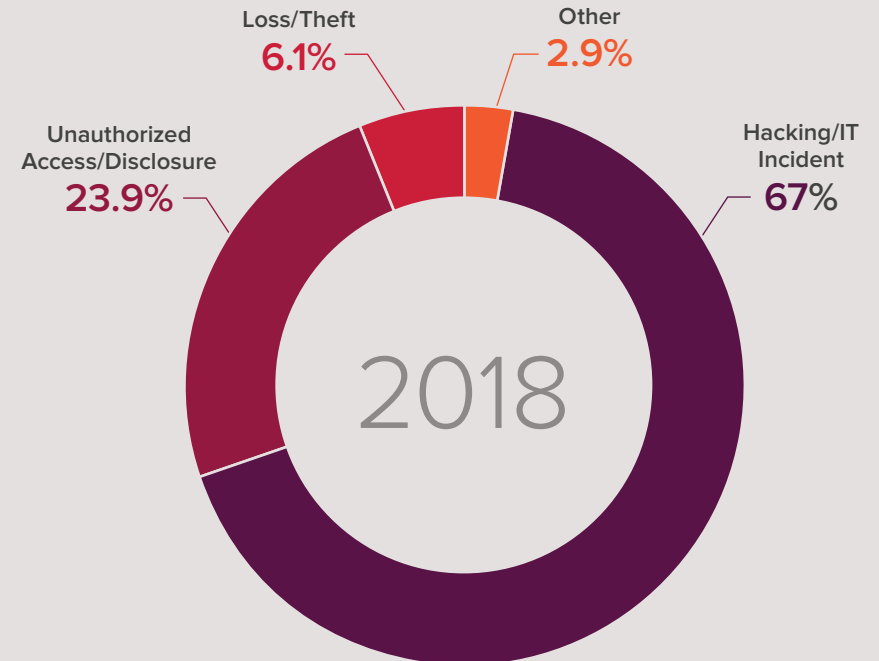
The number of breaches caused by lost and stolen devices has continuously decreased over the last five years—from 148 in 2014 to only 45 in 2018.

2018 at a Glance

Breach Causes

- Other **2.8%**
- Loss/Theft **15.5%**
- Hacking/IT Incident **45.9%**
- Unauthorized Access/Disclosure **35.9%**

2018

Individuals Affected

- Loss/Theft **6.1%**
- Other **2.9%**
- Unauthorized Access/Disclosure **23.9%**
- Hacking/IT Incident **67%**

2018

Hacking and IT incidents led to 45.9% of healthcare breaches in 2018. However, they impacted a disproportionate percentage of individuals relative to other breach causes. 67% of all persons affected by healthcare breaches had their information exposed by hacking and IT incidents. In other words, failing to protect data in IT environments can enable breaches of particularly large scales.

Breach Causes Year Over Year
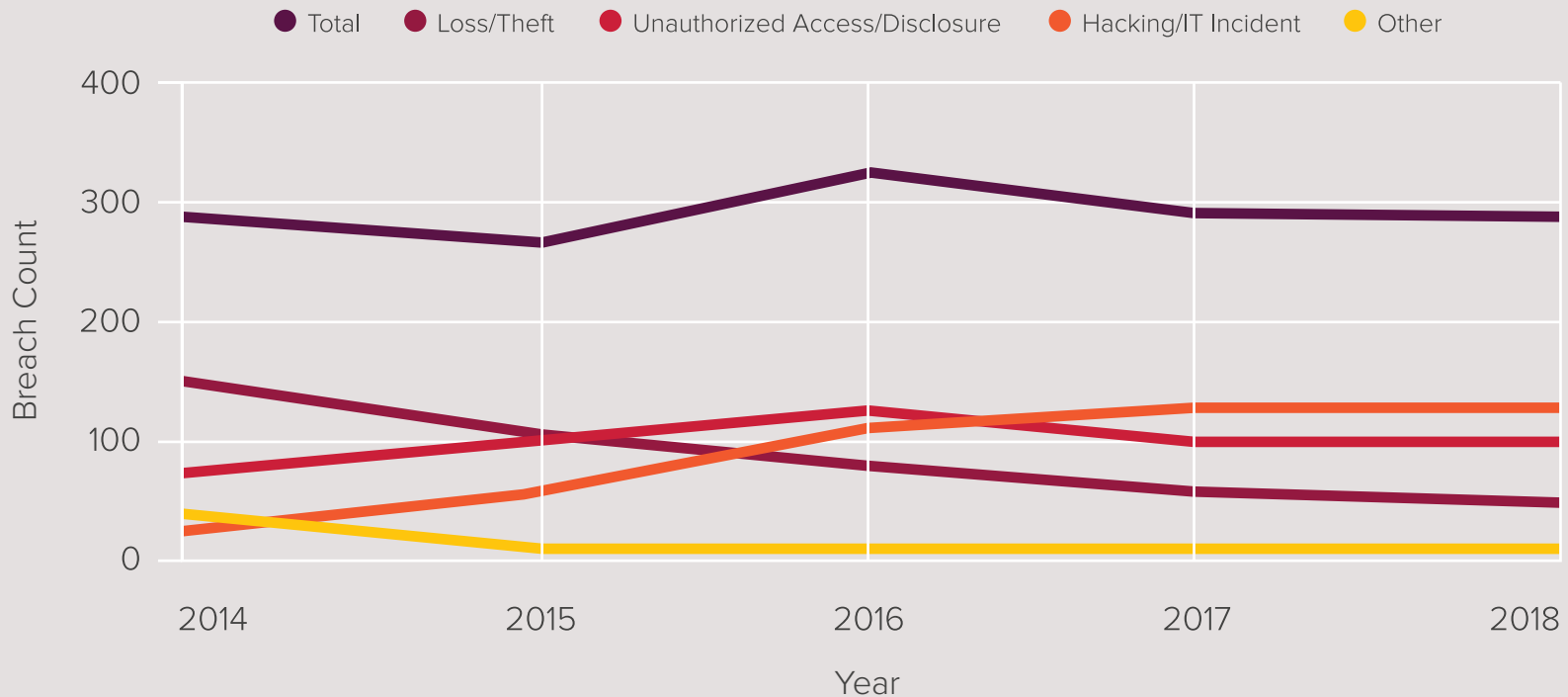
While lost and stolen devices were once the primary reason for breaches, they have since declined in prevalence. Uniquely, breaches caused by hacking and IT incidents have grown in frequency every year—even in years that saw the overall number of breaches decrease. This is because IT systems are attractive targets for criminals seeking to steal vast swathes of information (either for resale or for engaging in identity theft). Consequently, healthcare firms must leverage the appropriate technologies if they are to protect data in today's business world.
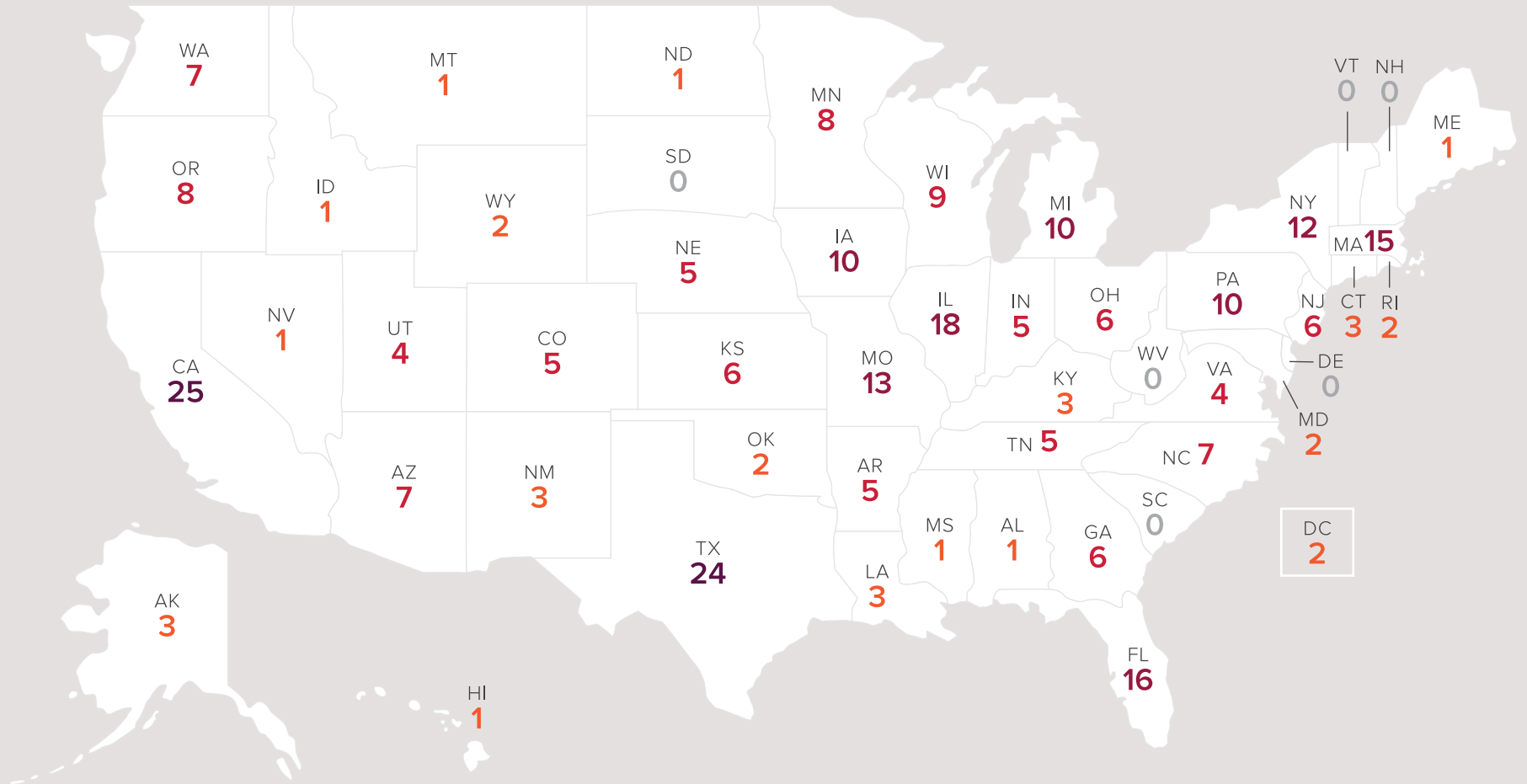
Individuals Affected Year Over Year
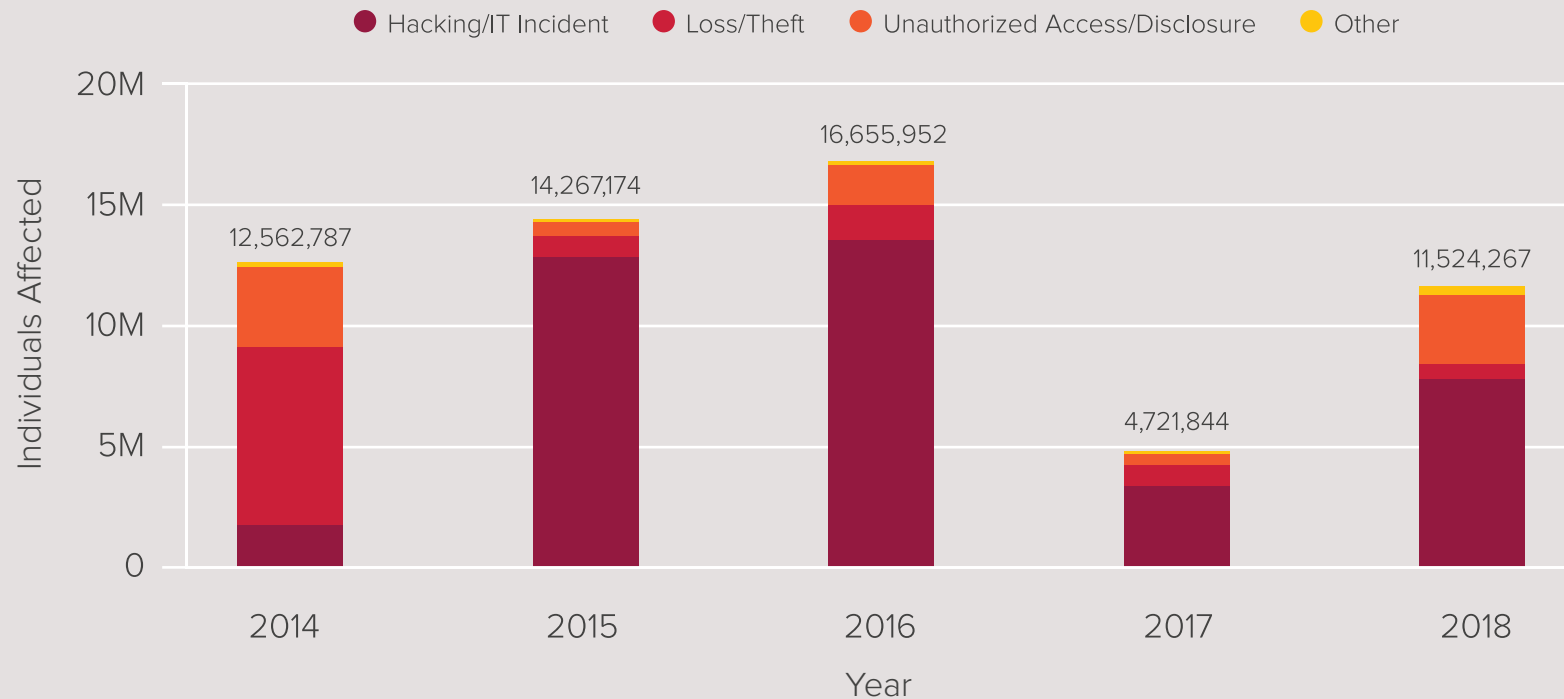
Despite the slight decrease in the number of healthcare breaches in 2018, the number of individuals affected during the year was still more than twice that of 2017. As can be seen in the accompanying chart, this growth in breach size was fueled by hacking and IT incidents as well as unauthorized data access and disclosure. This chart excludes the Premera and Anthem outlier mega-breaches from 2015, which would have brought that year's number of affected individuals to 111,812,172.
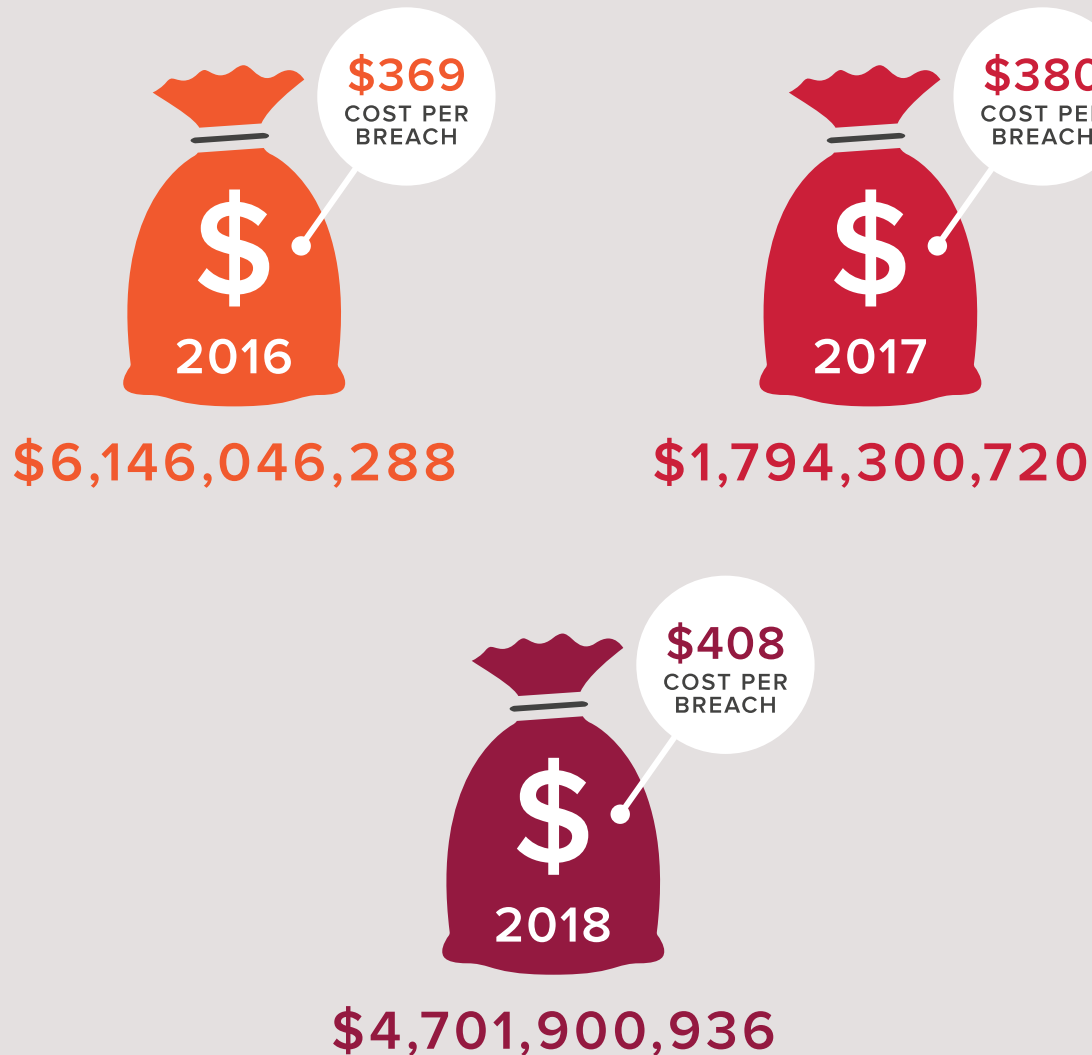
At 7,719,964, hacking and IT incidents affected more individuals than any other breach cause in 2018 (as they have each year since 2015).

Breaches by State

State	Breaches
WA	7
MT	1
ND	1
MN	8
VT	0
NH	0
ME	1
OR	8
ID	1
WY	2
SD	0
WI	9
MI	10
NY	12
MA	15
NV	1
UT	4
CO	5
NE	5
IA	10
IL	18
IN	5
OH	6
PA	10
NJ	6
CT	3
RI	2
CA	25
KS	6
MO	13
KY	3
WV	0
VA	4
DE	0
AZ	7
NM	3
OK	2
AR	5
TN	5
NC	7
MD	2
TX	24
MS	1
AL	1
GA	6
SC	0
DC	2
LA	3
AK	3
HI	1
FL	16

By far, California (25) and Texas (24) had the most healthcare breaches in 2018. This is consistent with state population (wherein California and Texas also rank first and second, respectively). When tested for correlation, state populations and the numbers of breaches shown above exhibited a strong, positive linear correlation (0.85), meaning that an increase in one is accompanied by an increase in the other. Some states clearly have more work to do when it comes to ensuring cybersecurity.

The Cost of a Breach in 2018

$369
COST PER
BREACH

2016

$6,146,046,288

$380
COST PER
BREACH

2017

$1,794,300,720

$408
COST PER
BREACH

2018

$4,701,900,936

Estimated Total Cost of Breaches

According to data from the Ponemon Institute, the cost per record for a healthcare breach amounted to $408 in 2018. This is a 7.4% increase from 2017 and a 10.6% increase from 2016. At $408, this cost was significantly higher than that of financial services, which came in second place at $206.

Compounding this problem is the fact that healthcare firms took a mean time of 255 days to identify breaches (the second longest for any industry) and a mean time of 103 days to contain them (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.

Appendix

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

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

*Excludes outlier mega-breaches

About Bitglass

Bitglass, the Next-Gen CASB 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