2014

Year of Mega Breaches & Identity Theft

Findings from the 2014

BREACH LEVEL INDEX

POWERED BY

gemalto
security to be free

SafeNet

BREACH LEVEL INDEX

THE NUMBERS

RECORDS BREACHED IN 2014

1,023,108,267

NUMBER OF BREACH INCIDENTS

1,541

BREACHED RECORDS INCREASE FROM LAST YEAR

78%

RISK ASSESSMENT SCORES 7.0 AND HIGHER - A SEVERE BREACH, POSSIBLY EVEN CATASTROPHIC

106

"More and more organizations are accepting the fact that despite their best efforts security breaches are unavoidable."

DATA RECORDS WERE LOST OR STOLEN WITH THE FOLLOWING FREQUENCY

- EVERY DAY 2,803,036
- EVERY HOUR 116,793
- EVERY MINUTE 1,947
- EVERY SECOND 32

INTRODUCTION

2014 YEAR IN REVIEW

Many information security experts will remember 2014 as the year of the big breaches—and with good reason. In addition to several high-profile hack attacks, the year included a number of lesser-known incidents that nevertheless resulted in significant theft of records, according to a comprehensive analysis of security breaches, conducted by Gemalto through data collected in its Breach Level Index.

To produce this report, **Gemalto**, a leading global provider of digital security solutions, has gathered extensive publicly-available information about data breaches throughout the world.

This data is aggregated in the **Breach Level Index**, a database the company maintains on data breaches globally. The information is analyzed in terms of the number of breaches, the number of data records lost, and data breaches by industry, type of breach, source and by country or region.

Clearly, the numbers were up in 2014. Data breaches totaled 1,540, up 46% from the 1,056 in 2013.

Even more dramatic was the rise in data records involved in the breaches. That jumped 78%, from about 575 million in 2013 to more than one billion in 2014.

From a time perspective, in 2014 some 2,803,036 data records were stolen or lost every day, 116,793 every hour, 1,947 every minute and 32 every second. So figure in about the time it took to read the previous sentence, about 400 data records would have been stolen or lost based on the 2014 data breach statistics.

And despite the growing interest of encryption technology as a means to protect for information and privacy, only 58 of the data breach incidents in 2014, or less than 4% of the total, involved data that was encrypted in part or in full.

But beyond the numbers was the social, economic and even political impact of the breaches. Some of the most high profile data breaches ever, including the ones against retailer Home Depot and entertainment company Sony Pictures Entertainment, occurred in 2014. And the year began with the Target breach of the previous year, another high-profile attack, still very much on the public's mind.

Many of the breaches in 2014 involved the theft or compromise of identifiable information, such as names, addresses and social security numbers. In comparison, many of the thefts of 2013 involved financial information such as credit card numbers.

Following are some of the most notable examples of data breaches in 2014, including the number of records stolen, type of breach and risk assessment score. The score is calculated based on factors such as total number of records breached, the type of data in the records, the source of the breach and how the information was used.

A score of 1 to 2.9 is minimal risk, 3 to 4.9 is moderate, 5 to 6.9 is critical, 7 to 8.9 is severe and 9 to 10 is catastrophic. The point of the scoring system in the Breach Level Index is to demonstrate that not all breaches have the same impact on organizations and amount of risk.

NOTABLE DATA BREACHES

Home Depot
10.0
109,000,000 records

The breach against the U.S.-based home improvement specialty retailer was a financial access attack that involved 109 million records and scored a 10.0 on the risk assessment scale. It was on of the largest attacks of the year in terms of records compromised. According to a statement by the company, its payment data systems were attacked. The files containing the stolen email addresses did not contain passwords, payment card information or other sensitive personal information, it said.

Korean Credit Bureau
10.0
104,000,000 records

The South Korean financial services provider suffered an identity theft breach that involved some 104 million records and scored a 10.0 on the risk assessment scale. CSO reported that the breach affected 27 million people, with compromised data coming from Web site registrations for various games and online gambling promotions, ringtone storefronts and movie ticketing. Records involved included names, account names and passwords, and resident registration numbers.

JP Morgan Chase
10.0
83,000,000 records

The U.S.-based financial services provider suffered an identity theft breach that resulted in 83 million records being compromised, scoring a 10.0 on the risk assessment scale. In a post on its Web site, the company said based its forensic investigation there was no evidence that customer account numbers, passwords, user IDs, dates of birth or Social Security numbers were compromised during the attack. However, contact information such as name, address, phone number and email address was compromised.

AliExpress
9.5
300,000,000 records

A critical but easily exploitable personal information disclosure vulnerability was discovered in the popular online marketplace owned by Chinese e-commerce company Alibaba.com, which affected its millions of users worldwide, according to The Hacker News. The account access breach involved 300 million records and scored 9.5 on the risk assessment scale. The reported vulnerability could allow anyone to steal personal information about hundreds of millions of AliExpress users without knowing their account passwords.

Sony Pictures Entertainment
6.5
47,000 records

Although it scored relatively low in terms of the number of records involved (47,000), the identity theft attack against the U.S. entertainment company was one of the most highly publicized hack attacks ever, garnering much attention because the U.S. federal government blamed the incident on North Korean attackers. The SPE breach scored a 6.5 on the risk assessment scale. But this does not take into account the loss from intellectual property theft from any videos/movies that might have been illegally obtained and released.

TOP SCORING BREACHES

2014 YEAR IN REVIEW

ORGANIZATION	RECORDS	TYPE	INDUSTRY	SCORE
HOME DEPOT	109,000,000	FINANCIAL ACCESS	RETAIL	10.0
J P MORGAN CHASE	83,000,000	IDENTITY THEFT	FINANCIAL	10.0
EBAY	145,000,000	IDENTITY THEFT	RETAIL	10.0
KOREA CREDIT BUREAU, NH NONGHYUP CARD, LOTTE CARD, KB KOOKMIN CARD	104,000,000	IDENTITY THEFT	FINANCIAL	10.0
BENESSE HOLDINGS	48,600,000	IDENTITY THEFT	EDUCATION	9.8
WEBSITES FOR ONLINE GAMES, MOVIE TICKETING AND RING TONE DOWNLOADS	27,000,000	IDENTITY THEFT	TECHNOLOGY	9.6
ALIEXPRESS	300,000,000	ACCOUNT ACCESS	RETAIL	9.5
KOREAN MEDICAL ASSOCIATION, ASSOC. OF KOREAN MEDICINE AND KOREAN DENTAL ASSOC.	17,000,000	IDENTITY THEFT	HEALTHCARE	9.4
NORTHWESTERN CITY OF VERDEN	18,000,000	FINANCIAL ACCESS	GOVERNMENT	9.3
NAVER	25,000,000	ACCOUNT ACCESS	TECHNOLOGY	9.3
KOREA TELECOM - KT CORPORATION	12,000,000	IDENTITY THEFT	TECHNOLOGY	9.3
SERBIAN STATE	7,276,604	IDENTITY THEFT	GOVERNMENT	9.1
INTERNET COUNTRY GERMANY	16,000,000	ACCOUNT ACCESS	GOVERNMENT	9.1

THE GEOGRAPHIC VIEW

NORTH AMERICA 76%

1,164 INCIDENTS

1,107	United States
57	Canada

Data breaches took place all over the world in 2014, but some regions were harder hit than others.

Easily at the top of the list in terms of the number of breaches was North America with 1,164 breaches, accounting for about three quarters of all breaches (76%). Those attacks involved more than 390 million records, or 38% of the total.

A distant second was Europe, with 190 breaches and about 79 million records. While Asia-Pacific had fewer breaches (129), it had the most number of records compromised: 545 million, or almost half of the total for the whole year.

Other regions that suffered attacks included Israel (17 attacks), the Middle East (15), Africa (8) and South America (6).

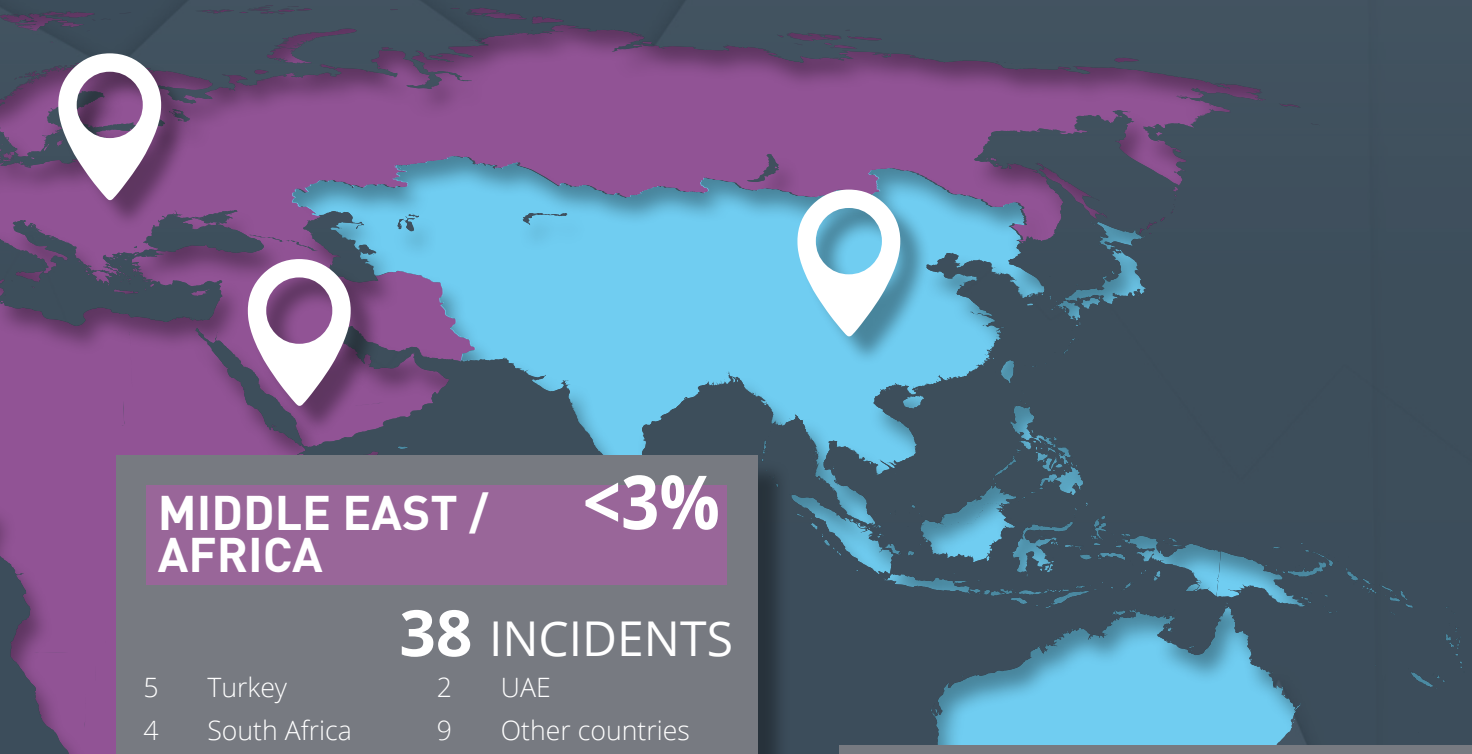
LATIN AMERICA <1%

12 INCIDENTS

3	Brazil
2	Dominican Republic
7	Other countries

Among individual countries, the United States had the most data breaches, with 1,107. That accounted for 72% among all nations worldwide. Next was the United Kingdom, with 117 (8%), Canada 57 (4%), Australia 30 (2%), Israel 17 (1%) and China 17 (1%).

THE GEOGRAPHIC VIEW 2014 YEAR IN REVIEW



MIDDLE EAST / AFRICA <3%

38 INCIDENTS

5	Turkey	2	UAE
4	South Africa	9	Other countries
2	Nigeria		

ASIA / PACIFIC 8%

129 INCIDENTS

30	Australia	4	Hong Kong
17	China	4	Malaysia
13	New Zealand	2	Azerbaijan
12	South Korea	2	Nepal
11	Japan	2	Singapore
9	Vietnam	2	Taiwan
7	India	7	Other countries
7	Pakistan		

EUROPE 12%

190 INCIDENTS

117	United Kingdom	3	Denmark
9	France	2	Poland
8	Ireland	2	Norway
7	Germany	2	Romania
6	Netherlands	2	Sweden
5	Belgium	2	Switzerland
3	Russia	2	Ukraine
3	Italy	11	Other countries

BREACH LEVEL INDEX

HOW THE INDUSTRIES COMPARE

RETAIL

While the **retail sector** might not have ranked at the top of the industry list in terms of the number of breaches, it had an astounding number of records exposed and included some of the most high-profile attacks of the year.

There were 176 data breaches among retailers, accounting for 11% of the total, which was up slightly from 8% in 2013. These attacks resulted in more than half a billion (567,316,824) data records being exposed. That amounted to

55%

of all the records involved in data breaches during the year, compared with 29% in 2013. The average records lost per breach was 3,223,391, versus 6,600,000 in 2013.

Among the top breaches in the industry were AliExpress with

300,000,000

records; eBay, with 145,000,000 records; Home Depot, with 109,000,000 records; Hannaford Bros., with 4,200,000 records; Michael's Stores, with 3,000,000 records; Staples, with 1,160,000 records; and Domino's Pizza, with 650,000 records.

As in the financial services industry, attacks against retailers put customers' financial data at risk. It's clear from the types of attacks in the retail sector that many were financially motivated. These types of breaches tend to receive a lot of publicity, partly because of the number of records involved but also because many people can relate to conducting business with retailers electronically.

FINANCIAL SERVICES

There were a total of 179 data breaches in the **financial services industry**, accounting for 12% of the total breaches last year. That percentage was down slightly from the year before, when it was 15%.

Finance companies had 205,175,846 data records compromised, representing 20% of the total records and up from 2013. The average records lost per breach was

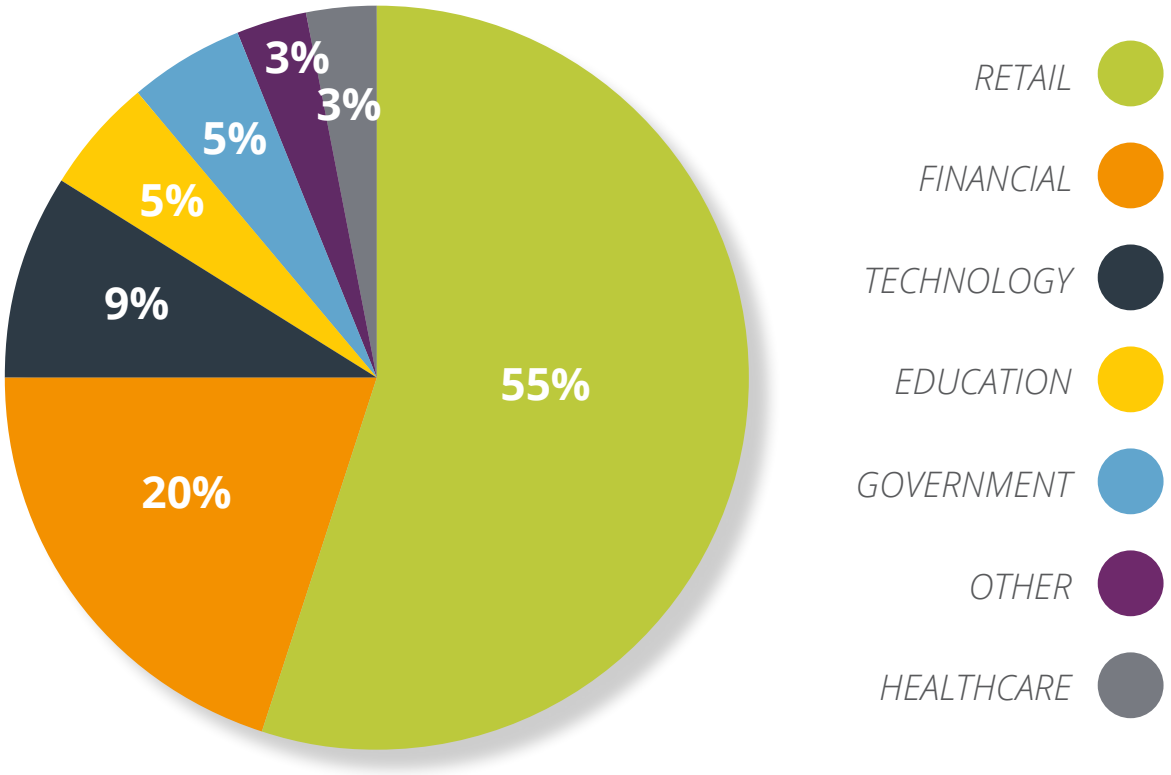
1,146,233

- up sharply from just 112,000 records in 2013.

Among the top breaches in the finance sector were the Korean Credit Bureau, with 104,000,000 records; JP Morgan Chase, with 83,000,000 records; and HSBC Bank in Turkey, with 2,700,000 records.

DATA RECORDS STOLEN/ LOST BY INDUSTRY

2014 YEAR IN REVIEW



TECHNOLOGY

The **technology industry**, which includes social media sites, had

134

data breaches in 2014. That accounted for 9% of the total, down from 11% in 2013.

The breaches against IT companies involved 96,493,092 data records, or 9% of the total. That percentage is down sharply from 2013, when it was 43%. Average records lost per breach in the industry was 720,097, compared with 5,700,000 in 2013. Top breaches in technology for the year included Naver, with an account access breach that exposed 25,000,000 records, and KT Corporation, with 12,000,000 records in identity theft.

The breach numbers have to be somewhat good news for an industry that is always concerned about attacks aimed at stealing intellectual property or launched for competitive reasons. Perhaps companies focused on technology are more proactive when it comes to deploying security tools to help protect their networks and data.

INDUSTRIES CONTINUED

GOVERNMENT

Government agencies and other public sector organizations experienced 264 data breaches, or 17% of the total, making it one of the most targeted industries.

These attacks involved 50,121,314 data records, or 5% of the total for all industries. Average records lost per breach was

189,853

The top breaches in government included Northwestern city of Verden, with 18,000,000 records exposed through a financial access attack; Serbian State, with 7,276,604 records through identity theft; and Internet country Germany, with 16,000,000 records through account access.

While the average number of records involved in each attacks was relatively low compared with financial services, for example, the total number of attacks was high.

EDUCATION

Educational institutions suffered 157 data breaches in 2014, or 10% of the total breaches for all industries. These attacks resulted in 51,377,801 data records being compromised, which accounted for

5%

of all the records stolen in attacks last year.

Among the top breach targets in the industry were the Benesse Holdings, with an identity theft attack involving 48.6 million records; Netherlands Primary School, with an identity theft attack involving 1 million records; and Maricopa County Community College District, with an identify theft attack that exposed 309,079 records.

As is clear from the statistics, breaches against educational institutions generally involve relatively small numbers of records.

HEALTHCARE

No industry experienced as many data breaches as the **healthcare** sector, which had

391

breaches in 2014. That amounted to one quarter of all the breaches reported for the year. As high as that percentage is, it's actually down from the 2013 share of 31%.

Healthcare organizations had 29,384,567 data records, or 3% of the total, compromised in these attacks. That percentage is down from 2% in 2013. The average records lost per breach for the industry was 75,152, compared with 49,000 in 2013.

Among the top breaches in healthcare were the Korean Medical Association, with 17,000,000 records exposed in an identity theft attack; Community Health Systems, with 4,500,000 records in identity theft; and the State of Texas Department of Health & Human Services, with 2,000,000 records in identity theft.

continued on page 12

DATA BREACHES THE WHO AND WHAT

2014 YEAR IN REVIEW

Among the key characteristics of security breaches—when it comes to addressing the attacks and making necessary changes to systems to avoid future attacks—are the type of breach and the source.

In many cases if organizations know how the attacks were conducted and by whom, they can take proactive steps to better protect themselves against similar intrusions and loss of data.

The Breach Level Index shows there were a variety of types of attacks and sources in 2014. While the sources of the attacks remained largely unchanged from those in 2013, the types of attacks were quite different from year to year in terms of frequency.

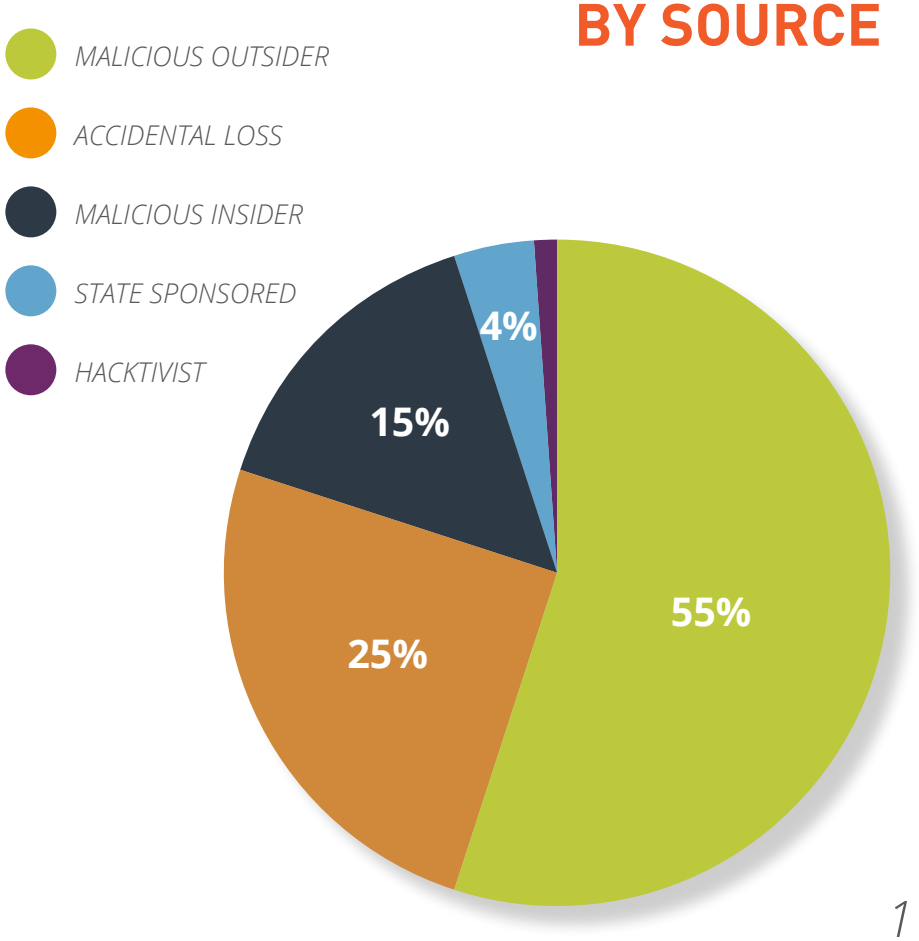
The most common type of source were **malicious outsiders**, who were involved in 854 breaches, or 55% of the total. The percentage is essentially unchanged from 57% in 2013. Clearly, this is by far the biggest threat organizations face today in terms of potential loss of data.

The next type of source, responsible for about one quarter of the breaches, was **accidental loss**. This caused 380 of the data breaches. In 2013, accidental loss accounted for 27% of the breaches. It's a bit perplexing that so many breaches could be caused by accident, and shows that companies need to do a better job of preventing mishaps that can lead to data loss.

Malicious insiders were the next most common source, responsible for 229 breaches. That was 15% of the total, quite similar to the 13% in 2013.

Next were **state-sponsored attackers**, who carried out 56 of the breaches, or 4%, in 2014. While it's a small percentage of the total,

NUMBER OF BREACH INCIDENTS BY SOURCE

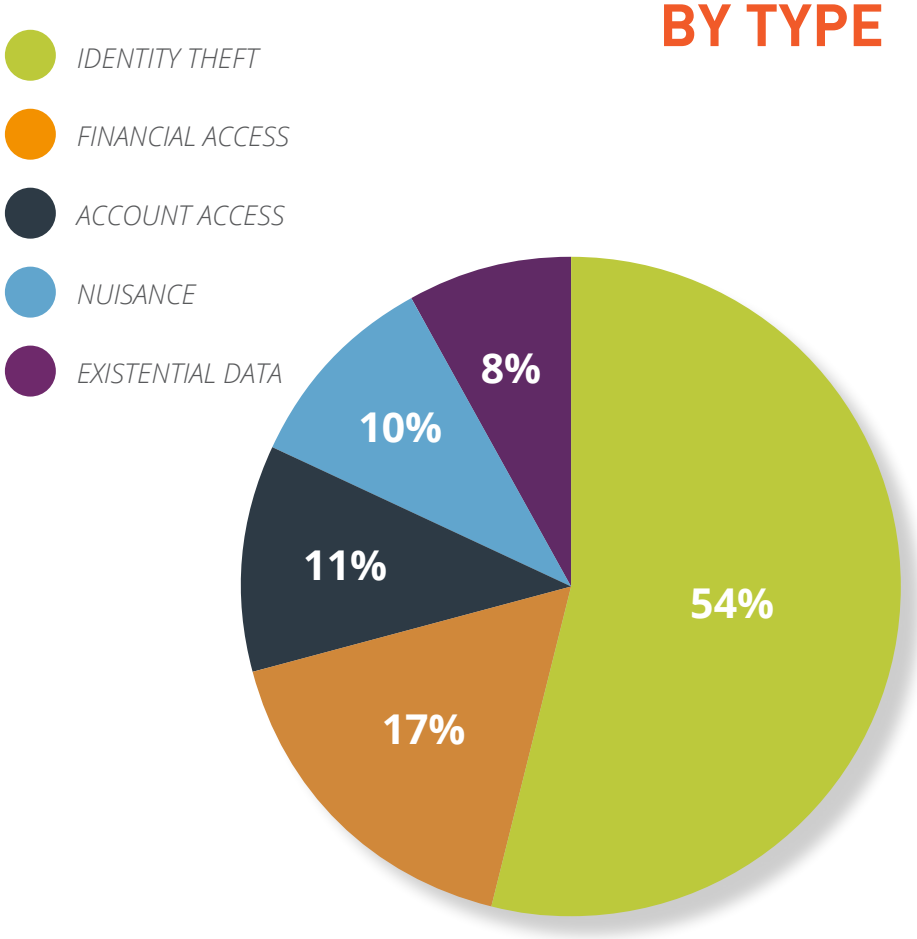


DATA BREACHES THE WHO AND WHAT

these sources increased from less than 1% in 2013. This is likely to be a continuing trend, as countries launch hacks against each other for political, economic, retaliatory or other reasons.

Hacktivists were the sources of just 19, or 1% of the attacks, with the percentage down from 2% the year before.

NUMBER OF BREACH INCIDENTS BY TYPE



The most common type of attack was **identity theft**. Organizations were hit with 827 of these attacks, which accounted for more than half of the total (54%). That's up dramatically from just 20% in 2013, which should be a concern for security operations. Clearly they need to do more to prevent identity theft.

The next most common type of attack was **financial access**, accounting for 261 or 17% of the breaches. That was down substantially from 50% in 2013. So these first two types of attacks basically switched places from year to year, which shows how dynamic and unpredictable the security environment can be.

Other types of attacks were **account access** (162 attacks or 11%, down from 28%); **nuisance** (157 attacks, or 10%, up from less than 1%); and **existential data** (134 attacks or 8%, up from 1%). The last two types represented fairly big increases and there deserve attention from security professionals.

continued from page 10

Exposure of records in healthcare is not only a security concern for these organizations; it puts companies at risk for regulatory non-compliance. For example, organizations in the U.S. must comply with the Health Insurance Portability and Accountability Act (HIPAA), which calls for the secure handling of patient information.

A NEW MINDSET FOR DATA SECURITY

2014 YEAR IN REVIEW

Breach Prevention Alone Has Failed

The 2014 Breach Level Index from Gemalto shows that data breaches are very much a growing threat for organizations. The number of records compromised is remarkable, considering the lengths many organizations go to in order to protect their data.

It's apparent that a new approach to data security is needed if organizations are to stay ahead of the attackers and more effectively protect their intellectual property, data, customer information, employees, and their bottom lines against data breaches in the future.

Security is consuming a larger share of total IT spending, but security effectiveness against the data-breach epidemic is not improving at all. Enterprises are not investing in security based on reality as it is; they're investing based on reality as it was: a bygone era where hackers were glory-seeking vandals, sensitive data was centralized, and the edge of the enterprise was a desktop PC in a known location. And in this reality, network firewalls and other network perimeter "breach-prevention" technologies were good enough. Unfortunately, **yesterday's "good enough" approach to security is obsolete** in an age where data is distributed across and beyond the enterprise, and hackers whether skilled criminals or insiders – both malicious and accidental – are a constant threat to data.

It's apparent that **a new approach** to data security is needed if organizations are to **stay ahead** of the attackers and **more effectively protect** against data breaches in the future.

There is nothing wrong with network perimeter security technologies – they are an added layer of protection. The problem is that many enterprises today rely on them as the foundation of their information security strategies, and unfortunately there is really no fool-proof way to prevent a breach from occurring. Alarmingly, market trends show that the lion share of organizations have no plans of changing this approach. According to IDC, of the $32 billion enterprises spent on security technology in 2013, more than 26% ($8.4 billion) was invested in network perimeter security.

A NEW MINDSET FOR DATA SECURITY

From Breach Prevention to Breach Acceptance

The Breach Level Index indicates that data breaches have been increasing in frequency and size over the last couple of years. So by definition, breach prevention is an irrelevant strategy for keeping out cybercriminals. In addition, every organization already has potential adversaries inside the perimeter. Disregarding these internal threats not only invites blatant misuse but also fails to protect against accidental carelessness. Even non-malicious behaviors such as bringing work home via personal email accounts, lost devices, storing data on USB drives and vendors unknowingly sharing network log-in credentials and passwords are a few examples of how easy it is to innocently leak sensitive data

In today's environment, the core of any security strategy needs to shift **from "breach prevention" to "breach acceptance."** And, when one approaches security from a breach-acceptance viewpoint, the world becomes a relatively simple place: securing data, not the perimeter, is the top priority. Securing the data is a challenging proposition in a world where cloud, virtualization and mobile devices are causing an exponential increase in the attack surface. Many organizations might be inclined to address this problem with a 'containment' strategy - limiting the places where data can go, and only allowing a limited number of people to access it. However, this strategy of "no" – where security is based on restricting data access and movement – runs counter to everything technology enables today. The mandate today is to achieve a strategy of "yes," which is built around the understanding that the movement and sharing of data is fundamental to business success.

From Breach Acceptance to Securing the Breach

It's one thing to change mindsets. It's another to implement a new approach to security across an organization. While there is no "one size fits all" prescription for achieving the "Secure Breach" reality, there are three steps that every company should take to mitigate the overall cost and adverse consequences that result from a security breach. **Control access and authentication of users. Encrypt all sensitive data** at rest and in motion, securely **manage and store all of your encryption keys**. By implementing each of these three steps into your IT infrastructure, companies can effectively prepare for a breach, and avoid falling victim to one.

It's not a question if your network will be breached, the only question is when. With the velocity of business increasing, new technologies constantly being deployed and new and sophisticated attacks regularly being launched, is it not inevitable that it is only a matter of time before your business is hacked. Learn more at:

www.securethebreach.com

The **year 2014** will be a tipping point for **data security** and **identity protection** because **data breaches** became more prominent in the **public consciousness.**

What's Your Score? Find Out At

BREACHLEVELINDEX.COM

Contact Us: For all office locations and contact information, visit www.gemalto.com and www.safenet-inc.com