F5 LABS

LESSONS LEARNED FROM A DECADE OF DATA BREACHES

Applications and identities are cyber attackers' primary targets, making way for the majority of breaches that are changing the way we view cyber security.

by Sara Boddy and Ray Pompon   NOVEMBER 2017

TABLE OF CONTENTS

TABLE OF FIGURES

EXECUTIVE SUMMARY

F5 Labs researched 433 breach cases spanning 12 years, 37 industries, and 27 countries to discover patterns in the initial attacks that lead to the breach.

We can only know about a small fraction of what's really going on, as companies often don't know when they have been breached. There's always a complicated mix of visibility, logging, monitoring and alerting, and communication that has many opportunities to fail.

VISIBILITY

- Do I know where all my key assets are?
- Do I know all the ways my networks connect outside of my organization?
- Do I have eyes and ears there? What are my visibility gaps?
- What am I not monitoring?
- Am I able to decrypt encrypted traffic?

LOGGING

- Am I capturing important events such as logins and access to key systems and data repositories?
- How robust is my logging?
- Can my logs be destroyed or tampered with?
- If my logs suddenly went silent, would I be alerted?
- If I were hacked, do I have the evidence throughout the entire attack path?

MONITORING AND ALERTING

- Am I getting alerts on the things that I can make decisions on?
- Did I get a new alert in a dashboard that no one has seen before?
- Did I get another email I wrote off as spam?
- Is someone starting an investigation?

COMMUNICATIONS MANAGEMENT

- Did a third party notify the company and it didn't get to the security team?
- How do those notifications reach me in a timely manner?
- Was that third party a researcher with a vulnerability disclosure, or worse, a copy of your data?

We also analyzed the primary root causes of the breaches, how that varied in breach remediation costs by industry, and the impact of these breaches on each data type breached on the global scale. The purpose of our analysis was to identify where organizations are most likely to be attacked in a way that will result in a breach so that efforts to mitigate attacks can be appropriately aligned.

These challenges result in only a small fraction of incidents being investigated and an even smaller amount of incidents being reported. That said, we think there are still valuable insights to be gained from these cases. Of the reported cases we analyzed, 79% of them had breach counts publicized, but only 49% had enough data to determine the initial attack vector, and only 40% a root cause. Finding a root cause can be tough. If you don't have enough of the visibility and logging controls in place, you may never know how an attacker got in, what they took, and how much. If a company doesn't know this information for a fact, there are many legal loopholes that excuse them from disclosing the incident at all. In some cases, this information is also held confidential due to law enforcement investigation—which is why we also reviewed the detailed court records of recent major breach cases.

Nevertheless, the number of breaches we know about, the types of data breached, and the total record counts and their impact is staggering. Here's a summary of the most impactful findings:

• **Applications were the initial targets in 53% of breaches.**

• **Identities were the initial targets in 33% of breaches.**

• **Breaches that start with application attacks account for 47% of the breach costs but only 22% of the total breached records, making application attacks the costliest.**

APPLICATIONS AND IDENTITIES ARE THE INITIAL TARGETS IN 86% OF BREACHES.

- Breaches that start with identity attacks account for 75% of the total count of records but only 24% of the breach costs, making them the most bountiful attack target for attackers, and the least impactful on breached businesses.

  > **The high record count plus low cost likely has something to do with the type of records breached. Email, usernames, and passwords are breached at the highest volume and are not yet regulated where costly disclosures are required. Yet these data elements are all an attacker needs to access business confidential systems, personal bank accounts, and so on.**

- Vulnerable forums installed on applications are the number one root cause of application attacks, followed by SQL injection.

- Out of 338 cases with confirmed breach data:

  > **11.8 billion records were compromised, an average of almost 35 million records per breach!**

  > **10.3 billion usernames, passwords, and email accounts were breached. That's 1.36 records per person on the planet, or 32 records per US citizen.**

  > **280 million social security numbers (SSNs) were breached, which is equal to 86.5% of the US population.**

- There have been so many breaches that attacker databases are enriched to the point where they can impersonate an individual and answer secret questions to get direct access to accounts without ever having to work through the impacted party.

- Dating and adult sites are compromised frequently, some of which contain the most deeply personal information about individuals, including sexual orientation and fetishes.

- Both definitions of "social engineering" are now applicable for cyberattacks:

DEFINITION OF SOCIAL ENGINEERING

SO·CIAL EN·GIN·EER·ING
/ ˌsōSHəl enjəˈni(ə)riNG/

1. the use of centralized planning in an attempt to manage social change and regulate the future development and behavior of a society.
   "the country's unique blend of open economics, authoritarian politics, and social engineering"

2. (in the context of information security) the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.
   "people with an online account should watch for phishing attacks and other forms of social engineering"

INTRODUCTION

Once the obscure and rare misconduct of hacker geeks, cybercrime now accounts for a substantial part of the illicit online activity designed to prey on society. In secret Internet darknets and forbidden chat rooms, international cybercriminals buy and sell stolen credentials and data. Rogue nation-states and anarchist groups routinely hire hackers to disrupt and infiltrate their enemies. The Pew Research Center published a report in 2017 noting that 64% of Americans have personally been victims of data breach.[1] The Internet Crime Complaint Center (IC3) operated by the FBI has reported 176% growth in reported cybercrime losses over the past five years, up from 525 million in 2012 to 1.45 billion in 2016.[2] The Identity Theft Resource Center reports that breaches increased in 2016 by 40% from the previous year.[3] We are living in an age of cybercrime that shows no signs of slowing down.

Who are these cybercriminals? How do they target their victims? What are they after? By looking at actual law enforcement intelligence and case investigations from the past five years, we can learn specific tactics and techniques used by cybercriminals to manipulate machines and humans alike. From this data we can derive actionable defensive measures for organizations based on likelihood of the target and, if properly addressed, help blunt the bite of cybercrime.

This is how you can improve your defenses within your own security programs—by understanding how attackers got in other organizations' systems and learning from their misfortunes.

[1] http://www.pewinternet.
org/2017/01/26/americans-
and-cybersecurity/

[2] https://pdf.ic3.gov/2016_
IC3Report.pdf

[3] http://www.idtheftcenter.
org/data-breaches.html

FIGURE 2

RISK LANDSCAPE

RISK

ASSET LANDSCAPE
What's being targeted in attacks? Users? Apps? The network?

IMPACT LANDSCAPE
What's the difference in impact based on the asset targeted?

CONTROL LANDSCAPE
Which security control was circumvented, failed, or didn't exist that led to the breach?
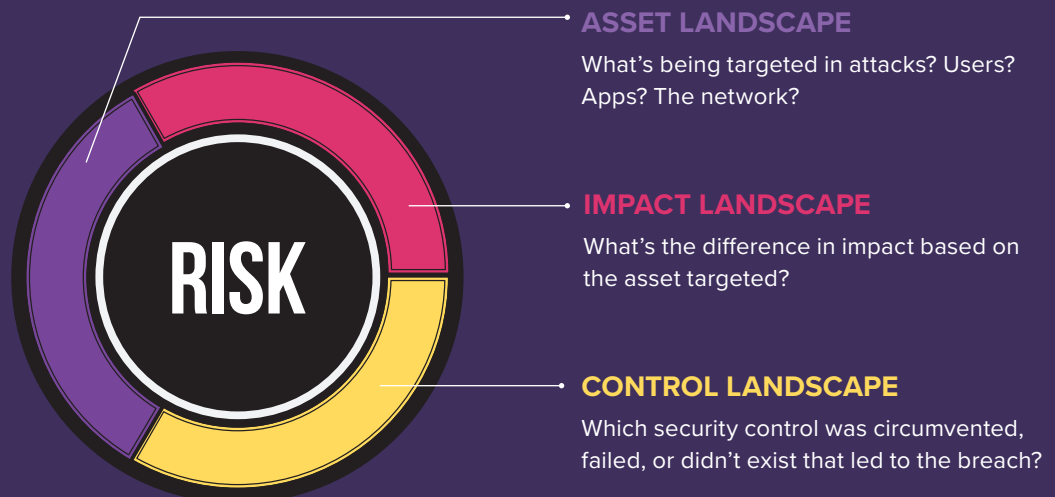
In this report we look at the following areas collectively to qualitatively and quantitatively determine the biggest areas of risk to all enterprises:

• **Asset landscape:**
  What's being targeted in attacks? Users? Apps? The network?

• **Impact landscape:**
  What's the difference in impact based on the asset targeted?

• **Control landscape:**
  Which security control was circumvented, failed, or didn't exist that led to the breach?

To draw a real-world attacker view of attacker targets, we examined the initial targets in the attacker's path that led to an impactful breach. We wanted to answer:

• **What does a targeted organization look like to an attacker?**

• **Where is the best place to focus security controls to blunt an attack?**

In addition, we examined the breaches by industry to determine if there were different attack or root cause patterns, or differences in breach costs by attack type to see if one was more impactful than another. Were there significant differences in the amount of records breached or ultimate cost to the business?

RESEARCH SCOPE

The scope of this research includes breaches in which either the number of records breached, incident cost to the business, or attackers was confirmed. We analyzed 433 cases that spanned 37 industries in 27 countries across North America, South America, Europe, the Middle East, Asia, and Africa.

CASES ANALYZED BY COUNTRY
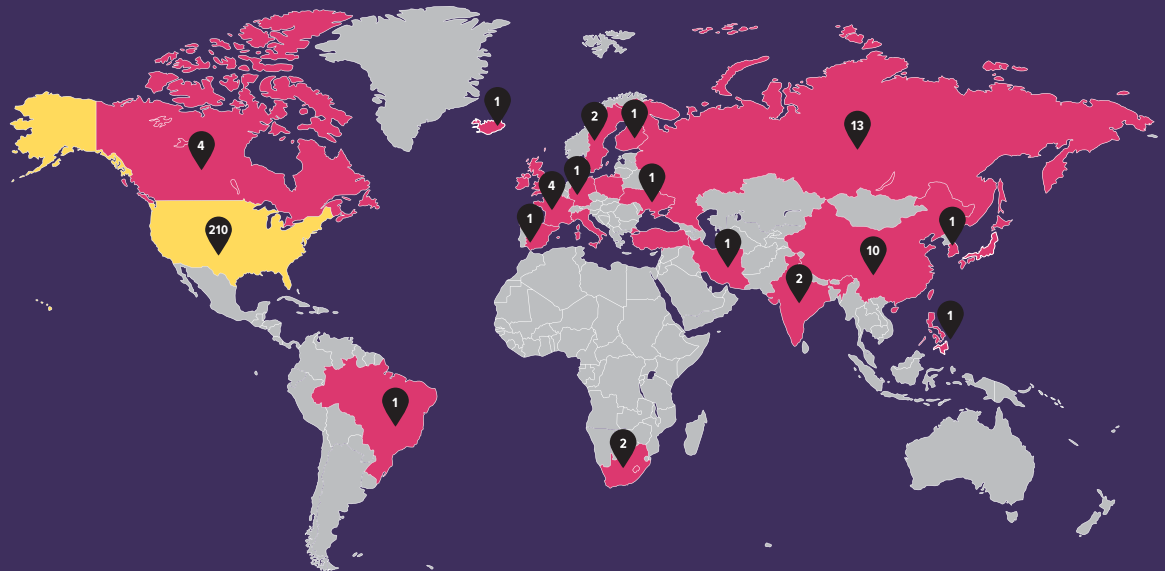
We evaluated cases to understand the attack plan, develop strong theories on the initial target and root cause—how attackers are "getting in"—and what the ultimate target was. We covered a wide range of attack types and targets to ensure our analysis was comprehensive.

We did not pick cases by date. The cases included in this report are heavily skewed towards the past three years because there is simply more and better data readily available in this time period. The cases that occurred between 2005 and 2010 are the largest, most harmful breaches in Internet history that have been reported in the most detail. We included them in this report because the data collected in these breaches is foundational to the rate of success attackers enjoy today. Big data allows attackers to find trends, optimize behavior, streamline and automate attacks, and therefore increase their cracking efficiency. Because all these root causes still exist today, these breaches show how we haven't gotten better at preventing breaches.

LIMITED LAWS = LIMITED DATA

Cases included in this report are heavily weighted on popular cases that were covered in the press. Some cases were pulled from government and researcher disclosure databases, and many were gleaned from news stories. Regarding the cases we pulled from media sources, there is a bias towards cases that were covered in the press, which are typically the larger, more sensational incidents.

FIGURE 4

CASES ANALYZED OVER TIME
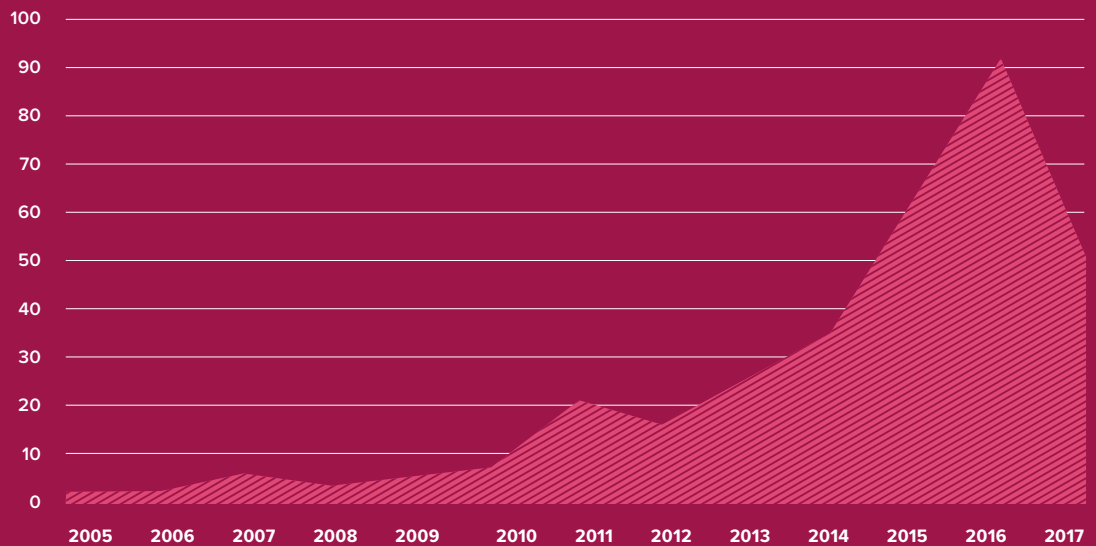
Getting a full population on all incidents globally is not possible at this point due to lack of awareness of breaches, and a lack of legal disclosure requirements. Globally, only three countries have comprehensive disclosure laws, meaning breaches must be disclosed to impacted parties, regardless of the encryption state of the data.[4]

4 http://www.
theworldlawgroup.com/wlg/
global_data_breach_guide_
home.asp

GLOBALLY, ONLY THREE COUNTRIES HAVE COMPREHENSIVE BREACH DISCLOSURE LAWS.

The US, Europe, and Southeast Asia have laws in place but don't require disclosure in all cases to affected victims. There are many caveats, including requirements for certain industries and not others; the requirement to notify law enforcement and not the individual; and lack of disclosure requirements to notify if the data was encrypted. The countries and US states with caveats in their laws are defined as "partial" in figures 5 and 6 below. Countries and US states requiring disclosure, regardless of data encryption status, are defined as "full" in figures 5 and 6 below.

FIGURE 5

GLOBAL STATE OF DISCLOSURE LAWS
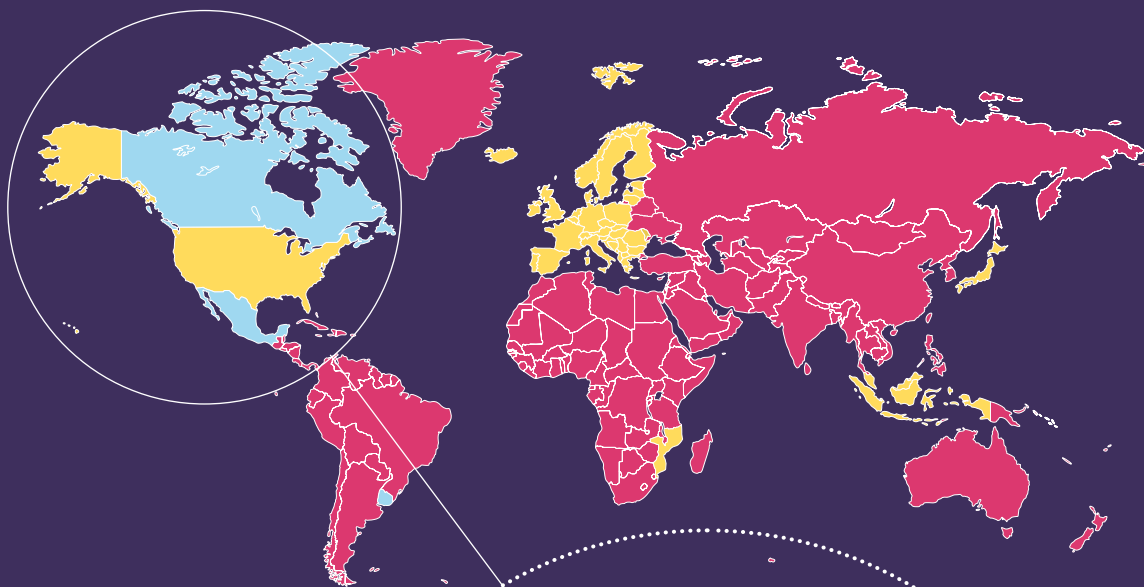
FIGURE 6

US STATES BY DISCLOSURE LAWS

FULL

NONE

PARTIAL
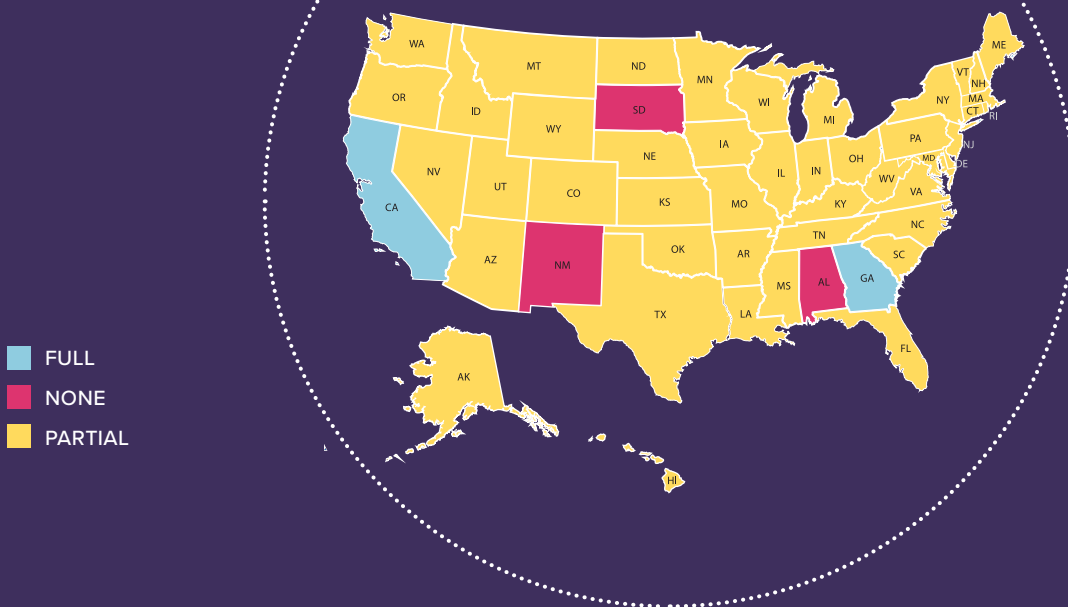
CASES ANALYZED BY INDUSTRY

The caveat on global breach and disclosure law is most apparent in the geo-disbursement of cases and industries, as shown in Figure 7. The more heavily regulated a country is, the more cases are available, which is why most of our examined cases come from the US, and in the healthcare and financial sectors. (Sources are listed in Appendix A.)

FIGURE 7

COUNT OF CASES BY INDUSTRY

■ Healthcare	■ Adult	■ Employment/Recruiting	■ Online Gambling	■ IoT Toys
■ Technology	■ Retail	■ Marketing	■ Review Site	■ Muslim Directory
■ Online Gaming	■ Entertainment	■ Public Utility	■ Background Check Firm	■ Pay-To-Click
■ Financial	■ News / Media	■ Airline	■ Bookmaker	■ Torrent Site
■ Online Forum	■ Online Dating	■ Automotive	■ Consulting	■ Virtual Pets
■ Government	■ Food	■ Data Collectors	■ Drugs	
■ Social Network	■ eCommerce	■ Engineering	■ Energy	
■ Cybercrime	■ Education	■ Non Profit	■ Intelligence	

SHOCKING BREACH FIGURES

In 338 cases, almost twelve billion records (11,768,384,080) were compromised. That's an average of 34,817,704 records per breach! To put that figure into perspective, the current world population is 7.5 billion, and the population of people online as of June 30, 2017 was 3.8 billion.[5] That's roughly 1.6 records breached per person in the world (just because you're not online doesn't mean your data isn't), or 3 records per person online that have been breached. We know this is a small portion of what has truly been breached.

[5] http://www.internetworldstats.com/stats.htm

433 BREACH CASES Breaches recorded between 2005 and 2017 **27 COUNTRIES** **37 INDUSTRIES**	**$2,756,254,700** Attacker profits **$3,288,337,000** Cost to breached organizations

Not surprisingly, email addresses, usernames, and passwords were stolen in the majority of the cases, as those datasets exists with every online account, totaling over ten billion records. That number is significant considering this data is all attackers need to get into an online account, and then get to even more of your data. In a lot of cases, the passwords were stored in plain text. Many organizations attempted to secure the passwords by hashing and salting them, but hashing mechanisms are relatively simple for advanced persistent threat actors to crack.

338 CASES Confirmed breaches with breach counts **11,768,384,080** Records compromised	**10,287,361,031** Emails, user names, and passwords **1,030,275,438** Credit card numbers **279,333,665** Social security numbers **547,331,712** Personal health information records

Every breach gives attackers more data to crack passwords with greater ease the next time around. Our data partner Lorkya tracks how quickly hashed passwords can be cracked. Loryka, as well as other researchers and attackers, can crack nearly every password (92% or more) within four to six hours after initiation. Their database of breached (unique) passwords, permutations of those passwords (users often don't change passwords completely but rather alter them slightly by using a different character at the end or replacing a letter with a number or symbol), and rainbow tables for hashes exceeds a trillion. However, because power efficiency and hash rates continue to rise with newly released hardware, leveraging these larger datasets becomes unnecessary as hashes are computed faster than lookups to tables.

HASHING MECHANISMS, ORDERED FROM WEAKEST TO STRONGEST TO CRACK: Based on modern Graphics Processing Units (GPU)	PBKDF2-HMAC-SHA1
	PBKDF2-HMAC-SHA256
	SHA256CRYPT
	PBKDF2-HMAC-SHA-512
	SHA512CRYPT
	SCRYPT (caveat—misuse at 1MB)
	BCRYPT (4KB)
	SCRYPT (>1MB utilization of memory)

All hashed passwords, no matter the mechanism, can eventually be cracked by a persistent attacker. However, it's worth pointing out that making it difficult or expensive will steer off the majority of attackers, so stick with the stronger hashing mechanisms.

Given the volume of breached credentials and the relative ease of cracking hashed passwords, it's reasonable to assume that if you reuse any of your online passwords or have been using the same credential pair (username + password) for an extended period, it's compromised.

THE PATH TO DATA: IDENTITIES ARE THE KEYS, APPS ARE THE GATEWAY

app
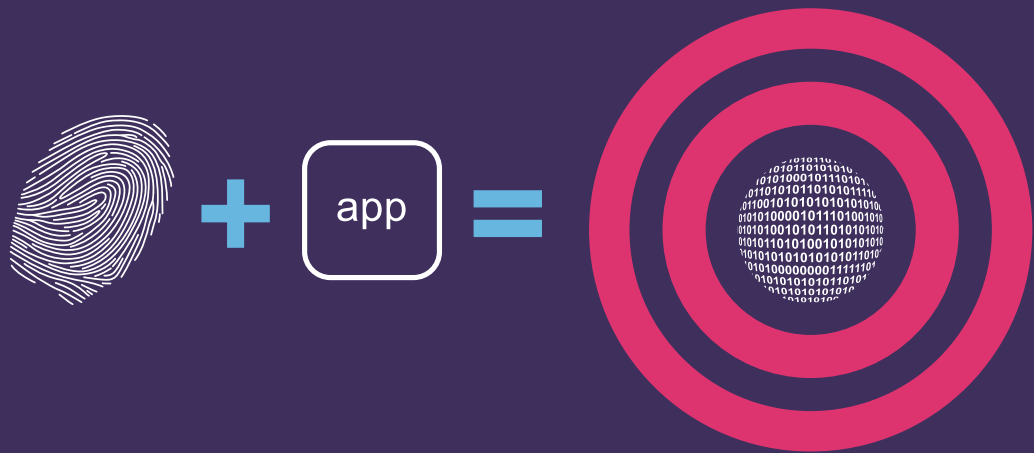
Even when attackers don't have your password, they can still get into your account; 3,360,563,907 secret question and answer records were compromised in the 338 cases we analyzed that included breach counts. That's not the number of questions, that's records regarding secret questions. Since websites typically collect between one and three questions and answers, the actual number of compromised secret questions is undoubtedly higher.

FRIENDLY REMINDER: CREDENTIALS ARE THE KEYS TO APPS, WHICH ARE THE GATEWAY TO YOUR DATA.

Over 1 billion (1,030,275,438) credit card numbers were stolen in 338 breaches. There were roughly 905 million cards issued in 2017.[6] Because these 388 cases spanned 12 years and included cards that have either been cancelled or are expired, it's unlikely the majority of these are still active. However, in many cases, the breached organization didn't know about the breach for years and only found out after their data was being sold online. This indicates attackers are compromising companies and sitting on the data for years before they use it. In some cases, attackers may have stolen more payment card data than they were able to discretely drain through fraud in a timely manner.

[6] http://www.cardrates.com/news/credit-card-companies/

Half a billion (547,331,712) personal health information (PHI) records were breached in the 338 cases we analyzed with breach counts. The current US population is 323 million. It's impossible to know the citizenship of the people whose records were breached because many of the breached companies operated globally and potentially had customers worldwide. It's sobering to see that the number of PHI records that have been compromised is larger than the population of the US.

Social Security Numbers (SSNs)—the most highly coveted, supposedly confidential, unique identifier to a citizen of the US. So important and uniquely identifying that you can't get a new one when it's compromised like you can a bank account, debit card, or online account. Yet, 275 million SSNs have been compromised, or 86% of the US population. (It's impossible to know the actual percentage of SSNs compromised without having the complete compromised dataset to de-dupe.)

275 MILLION SSNs HAVE BEEN COMPROMISED, OR 86% OF THE US POPULATION.

Speaking of unique identifiers you can't get rid of, 22 million biometric records were compromised in the cases we analyzed. Short of getting some fancy plastic surgery you see in a Hollywood movie, you're stuck with the fingerprint, facial features, and eyeballs you were born with (facial recognition software adjusts for age over time). The 22 million biometric records breached were from the US Office of Personnel Management (OPM) and the Philippine voter registration system, Comelec. Both cases cite "fingerprint" data, but do not give details. It's possible the records were hashes of the fingerprint based on biometric markers.

A startling amount of data regarding minors (anyone under the age of 18) has been compromised. Almost 36 billion (35,944,465) records of children's names, parent's names, dates of birth, age, gender, photos, voice recordings, IP addresses and, in some cases, phone numbers were included in the cases we analyzed. This isn't surprising, given that children are online as much as adults these days. This data in the wrong hands is frightening to parents. Data profiles of the newest generations are being built starting at a very young age whereas the profiles of those of us born before about 1980 (pre-Internet) started being built around the age of 18 using credit data. Prior to that, we had doctor and school records, but nothing was online then.

The point of profiling these crucial data types and comparing the breach quantity to the global population is to prove two points:

1. The question isn't who's been hacked anymore. It's who hasn't?
2. We now live in an assume breach world.

ATTACKS BY INITIAL ATTACK TARGET

In many cases, the initial target is not the ultimate goal. Robbers break through a window not just to get into a house but to find your valuables in a bedroom. In much the same way, a cyber attacker targets a user to get to an application, or the application directly to get to the data. Every attack plan requires getting through numerous controls to eventually get to the ultimate target. When investigating the root cause of the breach cases, we looked at the initial attack target to determine where the attacker struck first, and we looked to see if there was a pattern by industry.
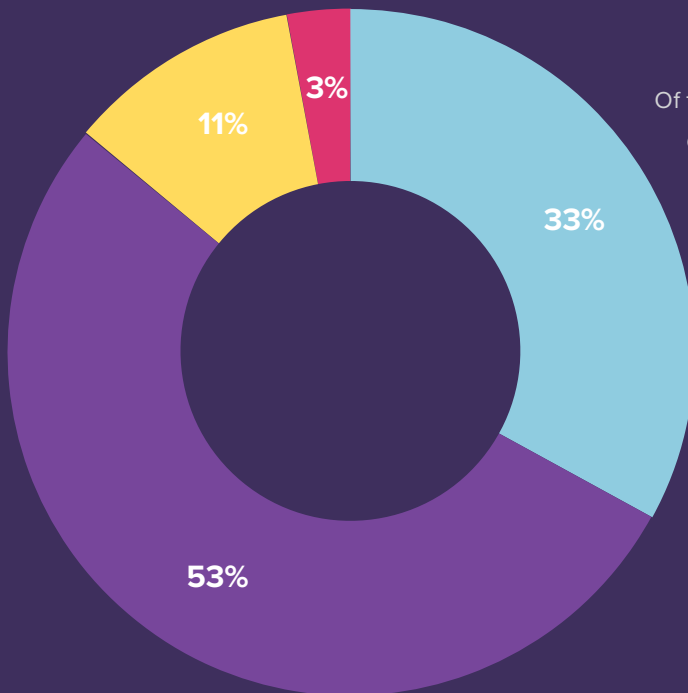
IDENTITIES ARE THE KEYS TO APPS

#1 TARGET

app

#2 TARGET

86% OF BREACHES INITIALLY TARGETED THE APPLICATION OR A USER/IDENTITY

FIGURE 9

CASES BY INITIAL ATTACK TARGET

Of the cases for which we were able to determine the initial attack target, applications were the first target in 53% of the cases, as shown in Figure 9. Identities were the first target in 33% of cases. Collectively, attackers started attacks either directly at the web application, or attacked a user for their identity in 86% of the cases.

- USER/IDENTITY
- APPLICATION
- PHYSICAL
- OTHER (VPN, ATM, DATABASE, DNS, NETWORK)

FIGURE 10

INITIAL ATTACK TARGET BY RECORD COUNT BREACHED

When looking at initial attack target by the number of records breached, identity attacks at 75% account for a disproportionate number of the total records breached (see Figure 10), indicating identity attacks are more successful for attackers (by data volume) than application attacks.
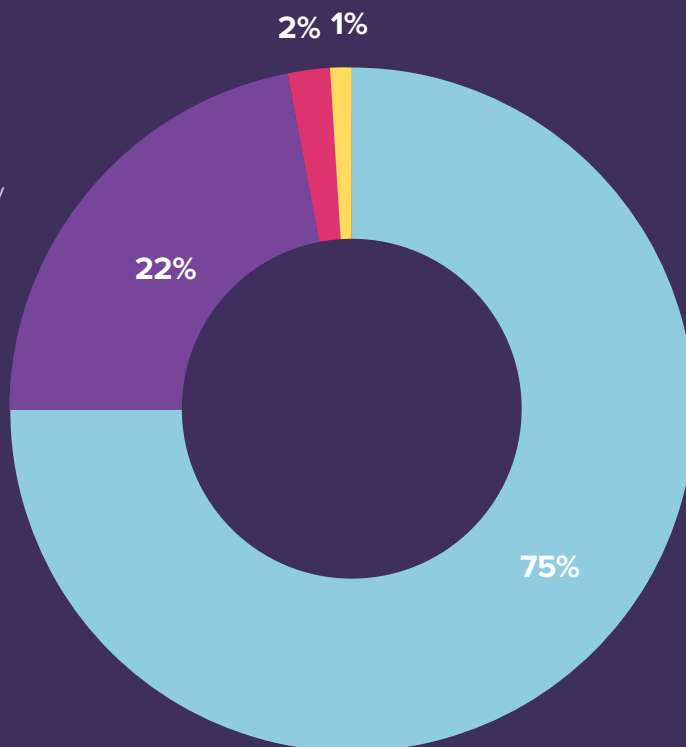
**FIGURE 11**

INITIAL ATTACK TARGET BY MONETARY DAMAGE TO BREACHED ORGANIZATION

However, when we looked at the initial attack target in relation to the cost of the breach to the organization, breaches that started with applications as their targets resulted in larger impact costs for the victim company, accounting for 47% of the total monetary damage. Identity attacks accounted for 24% of the total damage. It's likely that the majority of records breached in identity attacks are username, password and email addresses, which are not consistently regulated personally identifiable information (PII) datasets, and therefore wouldn't incur the same breach and disclosure costs.
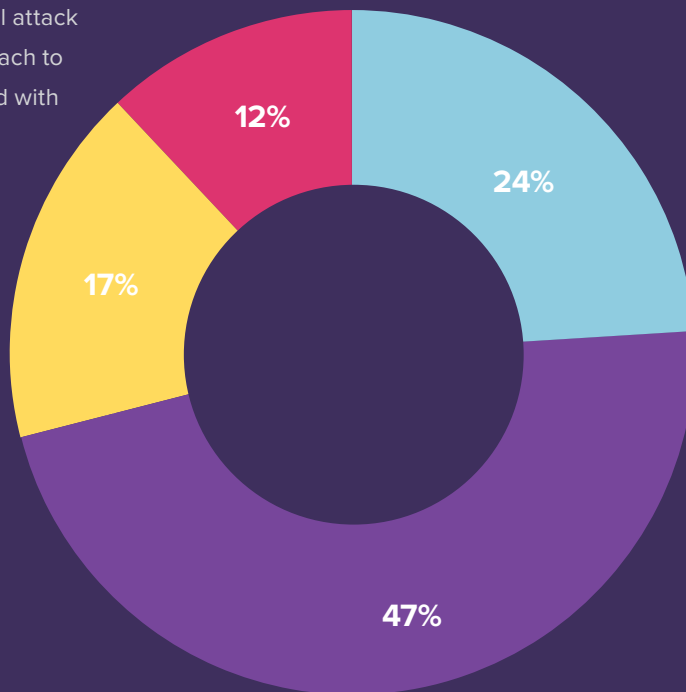
- USER/IDENTITY
- APPLICATION
- PHYSICAL
- UNKNOWN

When looking at cases by country where the initial target was defined, it's not surprising to see that the majority are within the US where there are simply more disclosures, and therefore more data.

FIGURE 12

CASES BY COUNTRY WITH INITIAL TARGET DEFINED

FIGURE 13

BREACHES BY ROOT CAUSE

EMPLOYEE MISTAKE
IMPROPER DISPOSAL
MALICIOUS INSIDER
MALICIOUS OUTSIDER
MALWARE
2FA FAIL
3RD PARTY
COMPROMISE
SPAM

- WEB APP VULNERABILITY
- PHISHING
- THEFT (BACKUP TAPE, DESKTOP, LAPTOP)
- UNAUTHORIZED ACCESS
- CREDENTIAL STUFFING
- OTHER
- DDOS
- MISSING PATCH
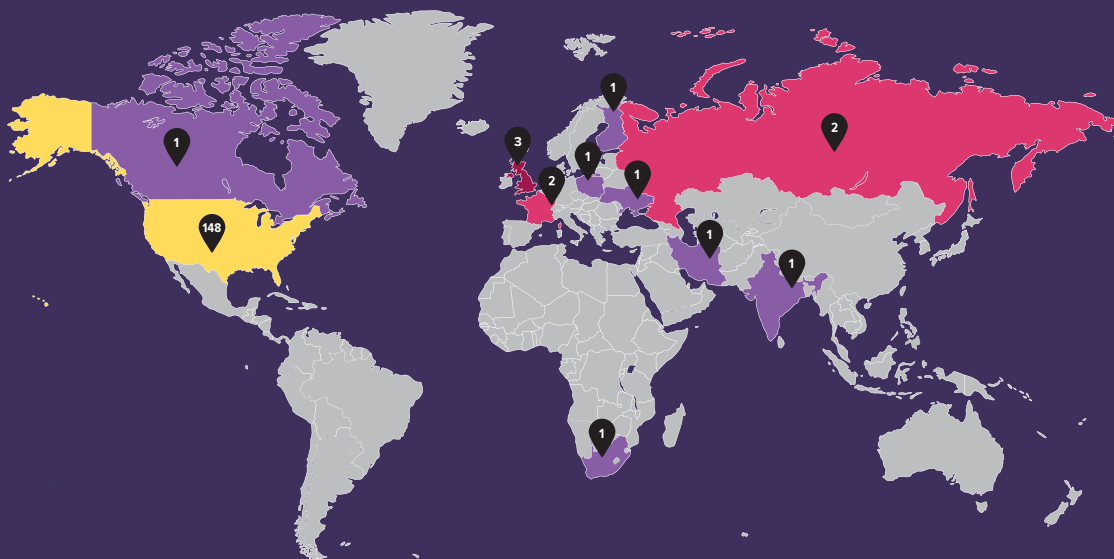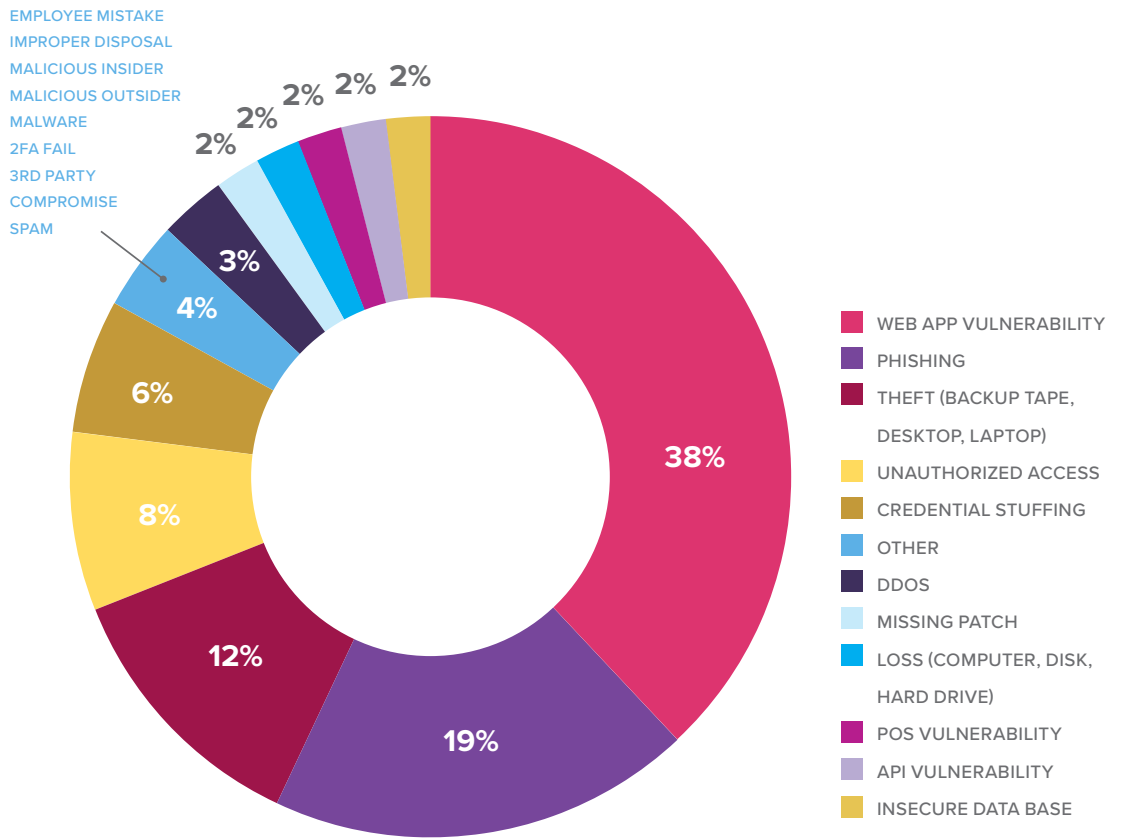- LOSS (COMPUTER, DISK, HARD DRIVE)
- POS VULNERABILITY
- API VULNERABILITY
- INSECURE DATA BASE

BREACHES BY ROOT CAUSE

We were able to identify a root cause of the breaches in 40% of the cases we analyzed. However, not all cases with a root cause disclosed the record count, breach cost, or attacker profits, so the stats in this section are based on a smaller subset of the data. As expected, the top two root causes, web application vulnerabilities and phishing, match the initial targets in the attack sequence: web applications and identities. Web application vulnerabilities were the number one root cause of the breaches analyzed at 38% of the total (see which type of web app vulnerabilities in the following section). Phishing was the second highest root cause at 19%. It's easy to trick a user into clicking malicious links or opening malicious files, no matter how many times you train them on what to look for.[7] Other identity attacks in the top 5 list of root causes include "unauthorized access" and "credential stuffing," which both likely started with a phishing attack or application exploit at some point prior where the data used in these attacks was collected.

Physical theft, in the third position at 12%, has been a primary root cause of breached data for decades. The physical theft cases in this research are heavily weighted in the healthcare industry where physical records are still common, as is physically transferring copies of records (tape, disk, hard drive, etc.) from one place to another.

Although "Insecure Database" is number 11 on the list, it's worth mentioning because, why on earth are databases directly connected to the Internet?! The growth of databases in the cloud is bringing an old, solved problem to light. Sixty-six percent of the exposed databases that were directly compromised (versus an app being exploited to get to a database) were the open-source MongoDB.

7 https://www.csoonline.com/article/2131941/security-awareness/why-you-shouldn-t-train-employees-for-security-awareness.html

WEB APPLICATION VULNERABILITY BREAKDOWN

Figure 14 details the different types of web application vulnerabilities behind the 38% of attacks where the root cause was a web application vulnerability.

FIGURE 14

WEB APPLICATION VULNERABILITY ROOT CAUSE BREAKDOWN

- FORUM (VBULLETIN)
- SQL INJECTION
- UNKNOWN
- FORUM (TYPE UNKNOWN)
- INJECTION VULNERABILITY
- FORUM (IP BOARD)
- WEAK AUTHENTICATION
- LOCAL FILE INCLUSION
- FORUM (MYBB)
- FORUM (PHP)
- FORUM (PHPBB)
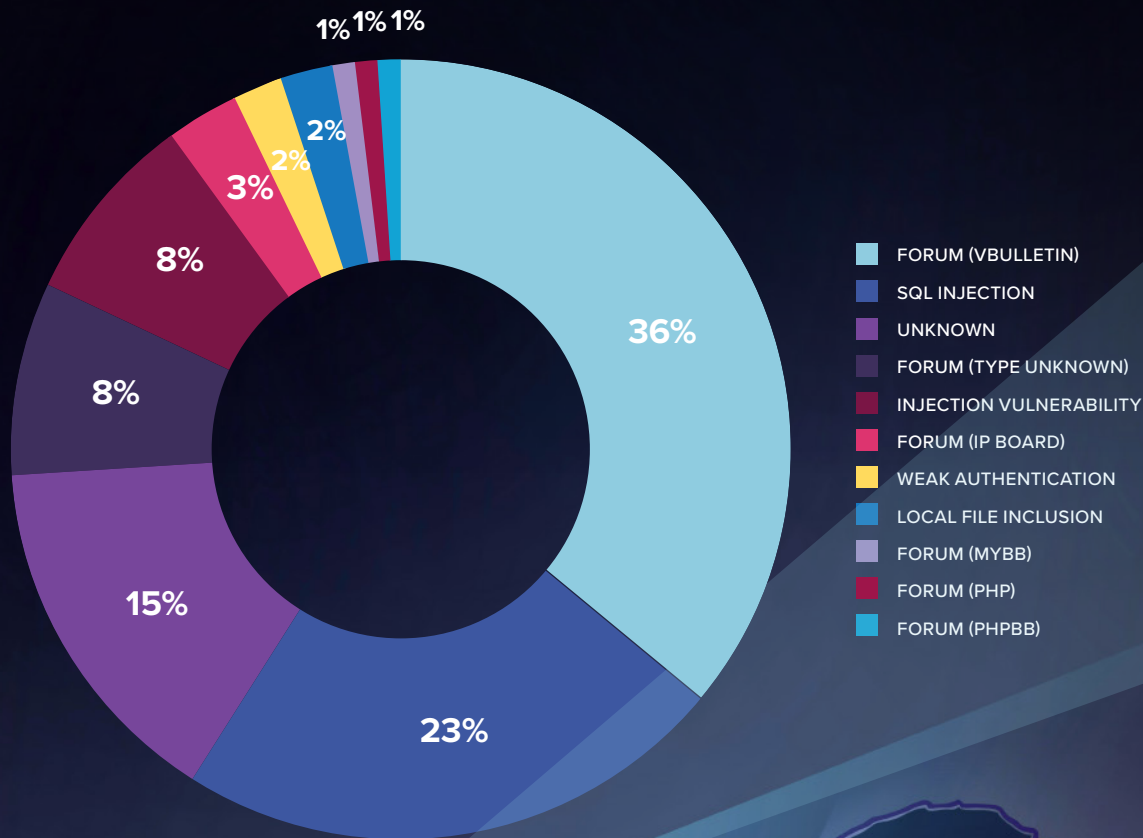
BAD FORM!

Forums, forums, forums.... Anyone who's been responsible for the security of several web applications will tell you that forums are the bane of their existence.[8] Forums provide user interaction features on websites that developers would otherwise have to code from scratch. By design, forums allow users to add content to a site and, without proper input sanitization, allow for malicious code to be injected.

A lot of forum software developers know their systems are heavily targeted and are getting better at automating updates that patch vulnerabilities relatively quickly. However, the more a forum is customized, the less able it is to benefit from auto updates, hence the large volume of forum exploits. vBulletin vulnerabilities were the root cause in 14% of cases for which we were able to identify a root cause, and accounted for 36% of the web application vulnerably category. And that's just specifically vBulletin. Scrolling further down the list is a generic forum vulnerability bucket for the breaches we know occurred through a forum, but we don't know the underlying forum product. Continuing down the list, more and more forum products show up as the root cause. In all, forum vulnerabilities account for 52% of all web application vulnerability root causes.

> # IN ALL, FORUM VULNERABILITIES ACCOUNT FOR 52% OF ALL WEB APPLICATION VULNERABILITY ROOT CAUSES.

THE SQL INJECTION FACE PALM

Second to vBulletin vulnerabilities is SQL injection. SQL injection is the most basic and damaging of all web application vulnerabilities because it allows an attacker direct access to your database. It's been around for decades and is an embarrassment to the security community that it still exists. It's an embarrassment because of how easy it is to find SQL injection vulnerabilities (seriously, it's really easy—you can run a free scan with SQLMap.org and within minutes have very confident results—the same results an attacker can get) and how trivial SQL injection vulnerabilities can be to fix within your web application code.[9] (It's not always a straightforward code fix, it's possible an entire site redesign would be required.) Not to mention the fact that there are free web application firewalls available that will automatically block SQL injection attacks so you don't have to find them or fix them. SQL injection vulnerabilities are an easily curable "disease" that we just can't seem to eradicate. Every time attackers find a SQL injection vulnerability, they compromise it within minutes and laugh all the way to the bank.

[8] https://f5.com/labs/articles/threat-intelligence/cyber-security/web-injection-threats-the-cost-of-community-engagement-on-your-site-22424

[9] https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet

RECORDS BREACHED BY ROOT CAUSE

1% 1% 1%

3% 3%

7%

18%

48%

18%

- PHISHING
- CREDENTIAL STUFFING
- WEB APP VULNERABILITY
- SPAM
- MALICIOUS OUTSIDER
- MISSING PATCH
- INSECURE DATABASE
- THEFT
- OTHER
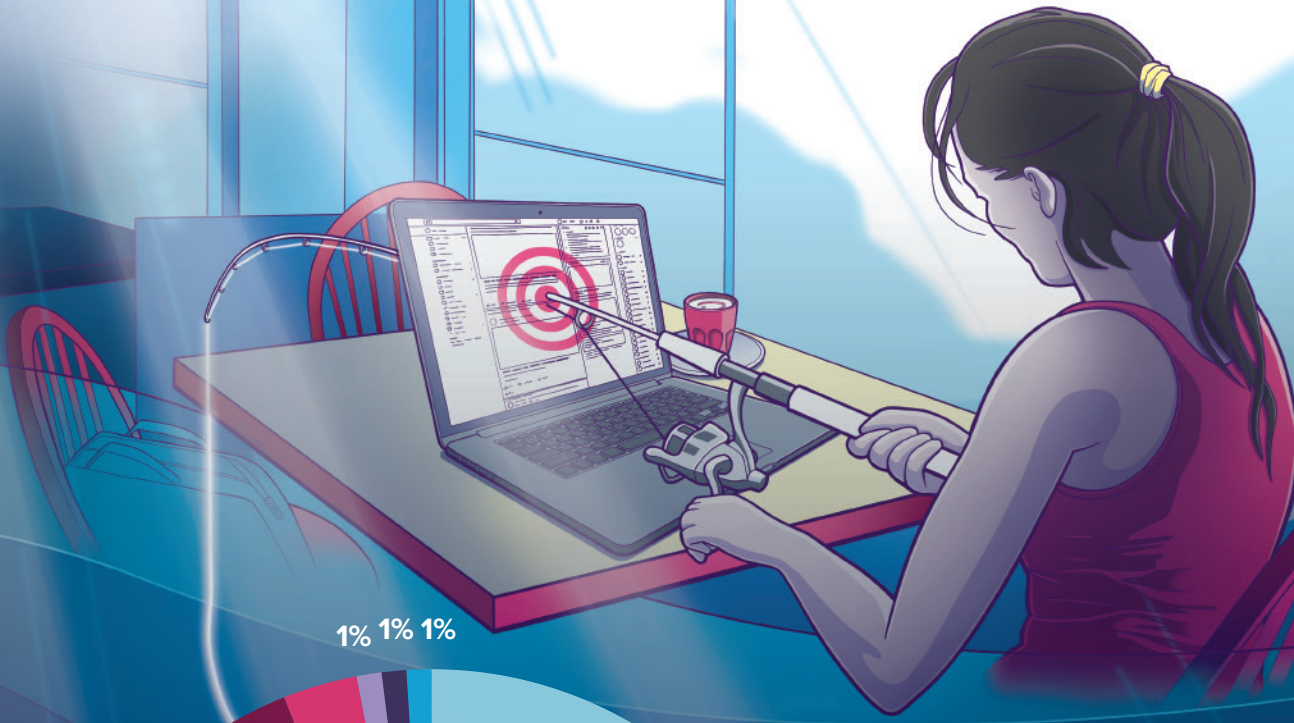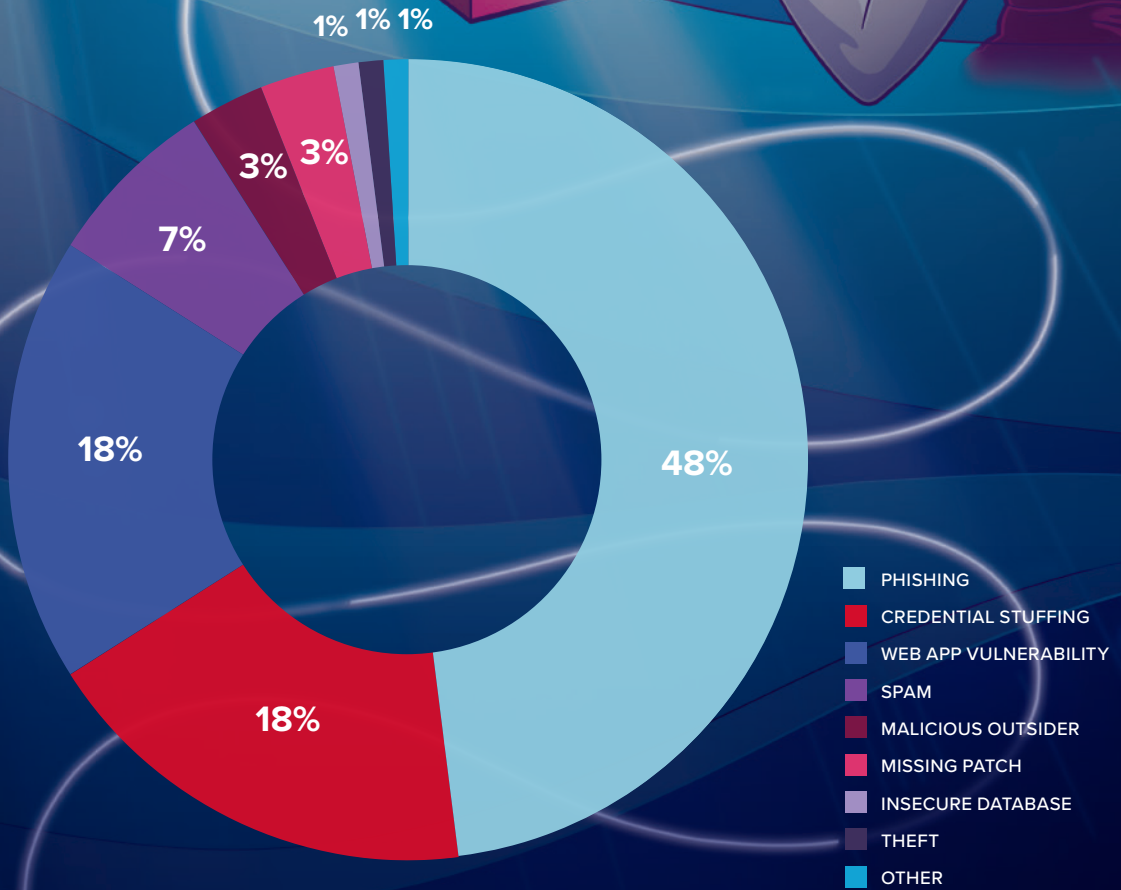
RECORDS BREACHED BY ROOT CAUSE

Phishing leads the list in number of breached records by root cause (just like "identities" leads the list in breached record count by initial attack target). Credential stuffing is the second root cause, which is the automated result of phishing and other attacks that collect identity data. Third on the list of most records breached by root cause is web application vulnerabilities. Specifically, forum vulnerabilities, SQL injection, and general injection vulnerabilities.

FIGURE 16

SOCIAL ENGINEERING CYBERATTACK POTENTIALS

Blackmail

Database Access

Application Access

Impersonation

Company Goodwill

Identity Compromise

Phishing Spear Phishing Whaling

CEO Fraud

Vishing

BEC

Credential Stuffing

Personal Reputation

Email Access

Malware

Click Fraud

Fraud

Voting

Protest

Fake News

Spam

Mind Control

Physical Harm Arrest

Democracy

Influence Purchases

Mindset Change

Brainwashing

WHAT'S THE PRICE OF DEMOCRACY?
2016 US PRESIDENTIAL ELECTION

PHISHING MADE POSSIBLE BY SOCIAL ENGINEERING

Phishing is a social engineering attack that is foundational to cyberattacks because of its ease of use and breadth of potential (see figure 16). It is the most successful attack in terms of driving the most records collected, and therefore has the greatest potential impact. In addition to records breached, it's breadth of impact is exhaustive, from tricking a user to opening a phishing email, collecting their credentials and eventually getting database access, to sending targeted content for the purpose of swaying opinions, such as the outcome of elections.

TYPICAL ATTACK PATHS

In most cases, applications are the primary entry point. Once an application vulnerability is exploited, attackers finds their way through the network to the data to steal. In the case of SQL injection, the data is delivered straight back to the attacker, which is why SQL injection is so popular for attackers.
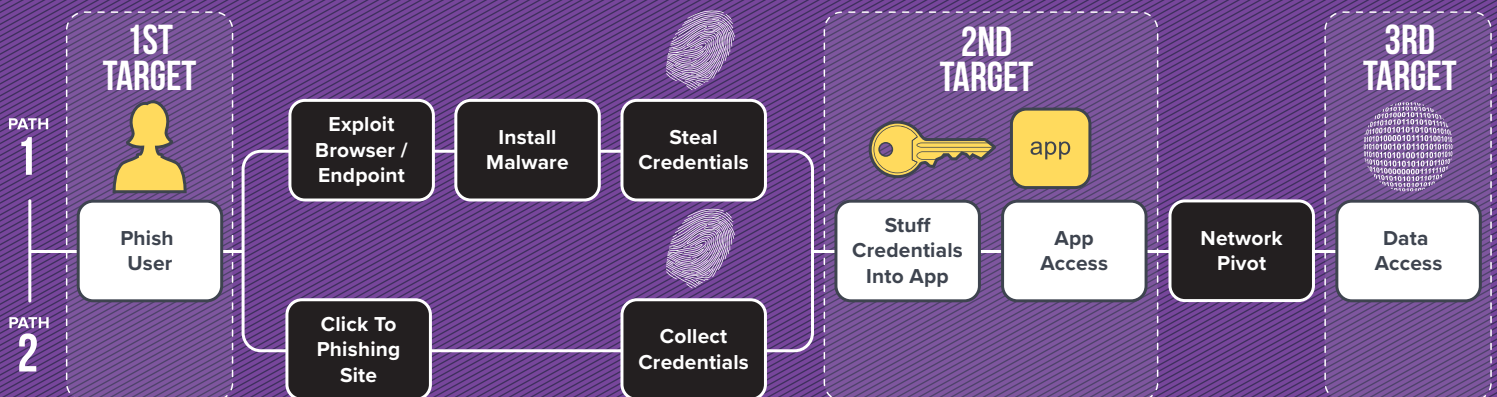
FIGURE 17

MOST PREVALENT ATTACK PATH: APPLICATION → DATA

1ST TARGET

app

App Access — Network Pivot — **2ND TARGET** — Data Access
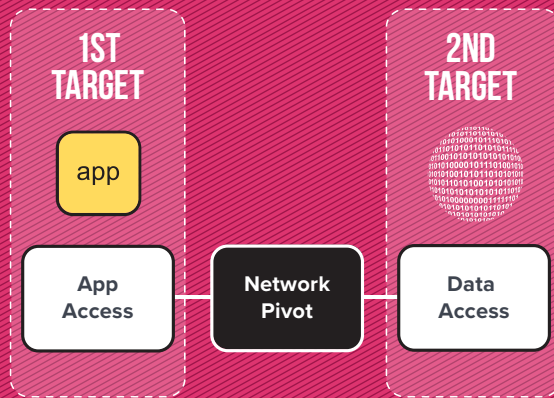
The second most prevalent attack path is by exploiting a user to hijack their identity credentials (see Figure 18). Once an attacker gets the user's identity, either by compromising an endpoint or collecting it directly through phishing, the attacker then has the keys to the app. With access to the app, the sky is the limit on what they can do. Depending on the stolen privileges of the compromised user, the vulnerabilities within the app may allow them to escalate privileges or connect directly to the underlying database.

FIGURE 18

SECOND MOST PREVALENT ATTACK PATH: USER → APPLICATION → DATA

1ST TARGET — Phish User

PATH 1: Exploit Browser / Endpoint → Install Malware → Steal Credentials

PATH 2: Click To Phishing Site → Collect Credentials

2ND TARGET: Stuff Credentials Into App → App Access

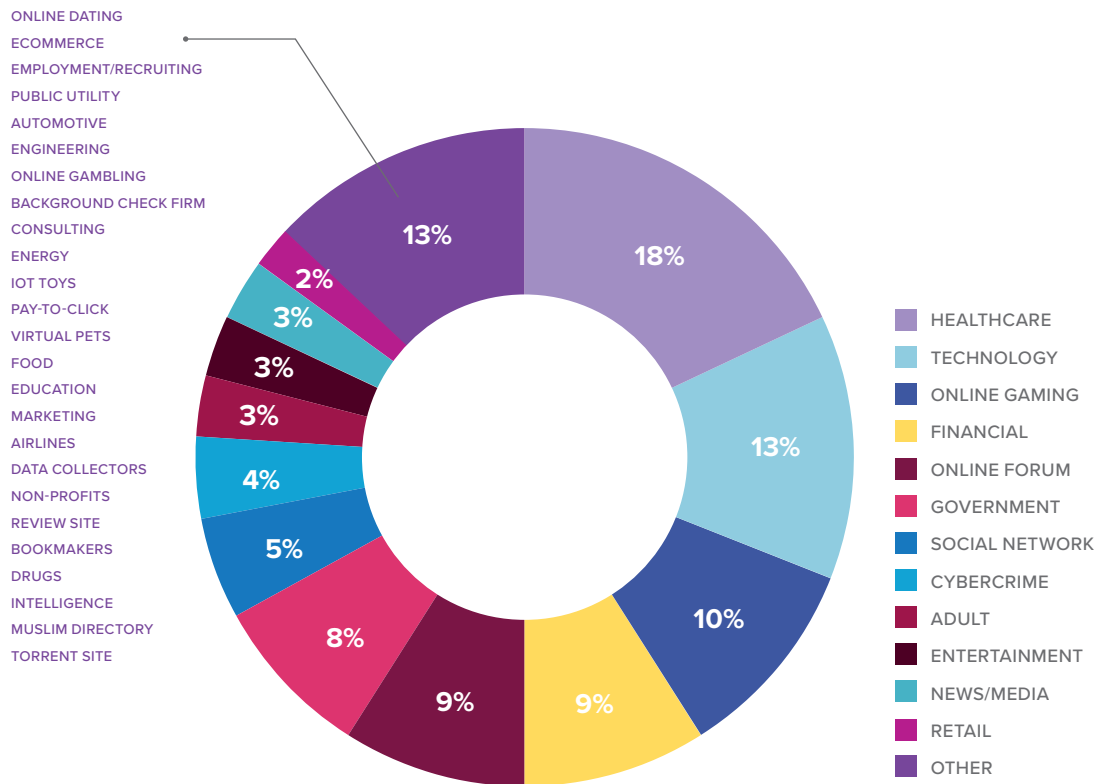Network Pivot — **3RD TARGET** — Data Access

CASES BY INDUSTRY

We grouped the cases by industry to see if there were different attack patterns for different industries. We identified 38 different industries across all of the cases we reviewed. Three industries, Technology, Financial, and Healthcare, are very high level and could be broken out further.

- **Technology** includes telecommunication and ISP companies, email providers, web hosting services, data center and co-location providers, data sharing platforms, intelligence firms, security product manufacturers, surveillance companies, etc.

- **Financial** includes banks, trading platforms, two of the three major credit bureaus, back-end payment processors, online transfer services, investment firms, stock exchanges, tax services, and accountants.

- **Healthcare** includes insurance providers, hospitals, pharmacies, etc.

After our analysis, the attack target patterns didn't vary noticeably when broken out into greater detail, so we kept them joined.

FIGURE 19

PERCENT OF CASES BY INDUSTRY

ONLINE DATING
ECOMMERCE
EMPLOYMENT/RECRUITING
PUBLIC UTILITY
AUTOMOTIVE
ENGINEERING
ONLINE GAMBLING
BACKGROUND CHECK FIRM
CONSULTING
ENERGY
IOT TOYS
PAY-TO-CLICK
VIRTUAL PETS
FOOD
EDUCATION
MARKETING
AIRLINES
DATA COLLECTORS
NON-PROFITS
REVIEW SITE
BOOKMAKERS
DRUGS
INTELLIGENCE
MUSLIM DIRECTORY
TORRENT SITE

- HEALTHCARE
- TECHNOLOGY
- ONLINE GAMING
- FINANCIAL
- ONLINE FORUM
- GOVERNMENT
- SOCIAL NETWORK
- CYBERCRIME
- ADULT
- ENTERTAINMENT
- NEWS/MEDIA
- RETAIL
- OTHER

Healthcare was the largest segment of breach cases. This was expected because the healthcare industry is governed by HIPAA, which requires organizations to disclose breaches no matter how small. This creates a larger volume of breach data in the healthcare industry compared to other industries. But, the healthcare industry has close to the lowest number of records breached, and the lowest breach cost of any industry.

A high quantity of breaches (indicating industry wide security issues), with an overall low impact can be a dangerous mix as it sets a "we can sustain a breach" tone. Another reason for this could be that healthcare providers simply have less unique data. One website could easily have three different records for one person (how many times have you reset your username and password on likely dozens of accounts?), whereas people typically go to the same doctors most of their lives, only have a few different insurance provider options throughout their lives, and only visit hospitals and specialty clinics when they are seriously ill or hurt. To put things in perspective, Anthem's major breach that impacted two-thirds of Americans is included in the healthcare figures, and personal health information (PHI) only accounted for 5% of the data records breached in the cases we analyzed. There are literally hundreds of technology websites that have more data records than Anthem.

Second to healthcare is technology companies followed by online gaming, and financial firms. Collectively, they account for 50% of the cases we analyzed.

When looking at the industries by breach impact cost (Figure 20), the results are drastically different. Retail accounts for 3% of the total cases, but 49% of the total damage costs. Government accounts for 8% of the cases, but 17% of damages. Technology is relatively flat in ownership of cases with damages at roughly 14%.

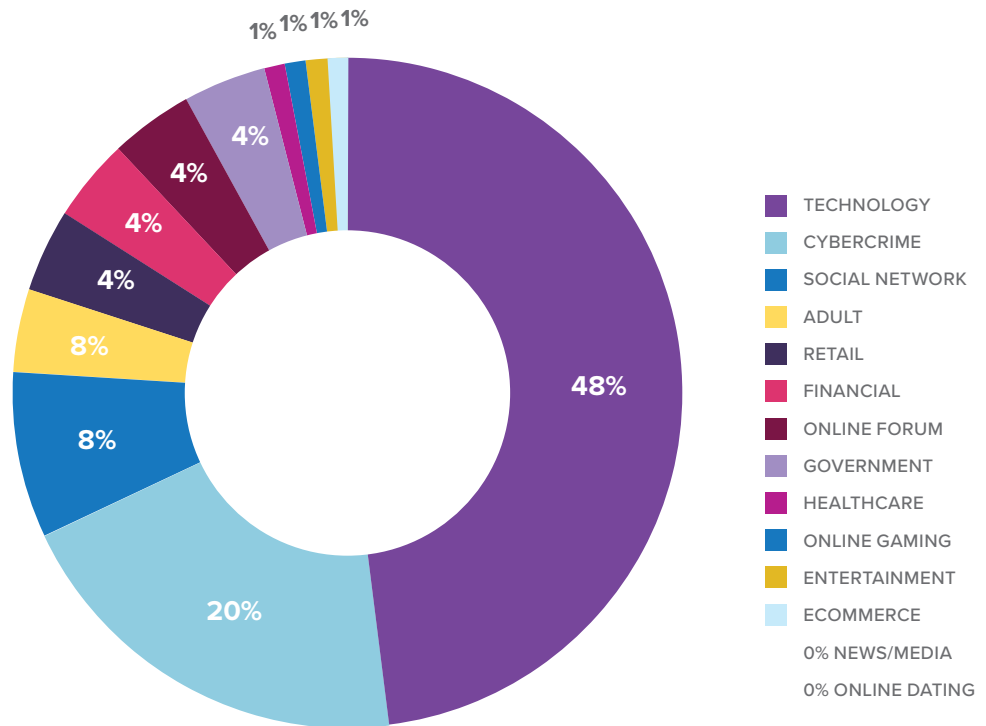## PERCENT OF BREACH COST BY INDUSTRY

RETAIL
GOVERNMENT
TECHNOLOGY
FINANCIAL
ONLINE GAMING
HEALTHCARE
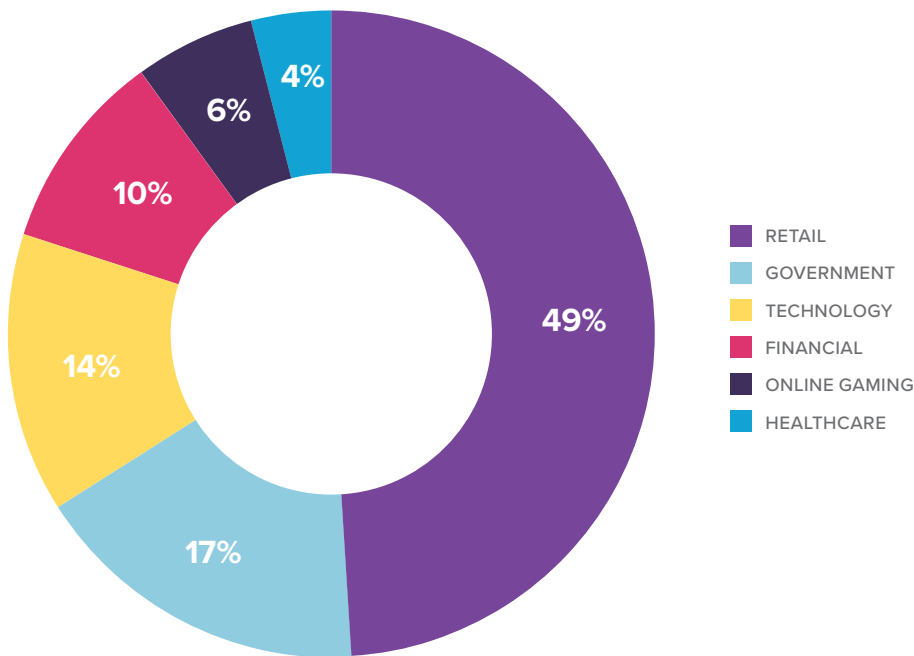
When looking at the number of records breached by industry, the technology sector accounts for almost half of all breached records, yet only 14% of the breach damages. Attacker-on-attacker cybercrime, in which attackers attack each other to steal previously stolen data, accounts for 20% of the breached records, but obviously none of the victim damages. If attackers are caught (which has a very low probability), they pay in jail time.

Social networks are ranked third in number of records breached by industry, yet they account for 0% of damages (and they represented only 5% of the total cases). We only found one social network breach with an associated cost of breach damages, which was LinkedIn, estimated at $1 million (on the high end), which is .03% of the breach damages we collected.

FIGURE 21

COUNT OF RECORDS BREACHED BY INDUSTRY

- TECHNOLOGY
- CYBERCRIME
- SOCIAL NETWORK
- ADULT
- RETAIL
- FINANCIAL
- ONLINE FORUM
- GOVERNMENT
- HEALTHCARE
- ONLINE GAMING
- ENTERTAINMENT
- ECOMMERCE
- 0% NEWS/MEDIA
- 0% ONLINE DATING

DETAILS OF RECORDS BREACHED

Across the 338 cases with confirmed breach counts, we tracked the following data types and counts:

FIGURE 22

COUNT OF RECORDS BREACHED PER TYPE

RECORD TYPE	COUNT
TOTAL NUMBER OF RECORDS	11,768,384,080
Email	10,287,361,031
Password	9,133,934,569
Username	6,692,756,532
Security Q&A	3,360,563,907
First and last name	2,831,597,520
IP address	1,463,245,336
Date of birth	1,428,332,263
Address	1,316,836,869
Phone number	1,095,332,440
Credit/Debit cards	1,030,275,438
Gender	582,454,862
Personal health information	547,331,712
Social security numbers	279,333,665
Credit score	166,869,797
Bank account number	103,456,959
Minor data (child's name, DOB, age, gender, photos, voice recordings, IP's)	35,944,465
Passports	22,466,605
Government issued ID	22,238,000
Biometric data	22,228,605
*Other	1,349,127,061

*Other: Includes data breached in conjunction with email and/or username, password, first and last name, broken into two categories; personal data and business data.

PERSONAL DATA
Account balances, payment histories, and payment methods
Email messages, IM identities, chat logs, private messages
Recovery email addresses
Browser user agent details
Website activity
Geographic locations, time zones
Travel habits
Personal data of "high profile" accounts (public figures)
Income levels
Purchases, buying preferences, financial investments, net worth
Political donations, charitable donations
Home ownership status
Employers, job titles, employment histories of current and former customers, work habits, career levels, professional skills, years of professional experience
Drinking habits, drug habits, smoking habits
Age, age groups
Education level
FAFSA student loan apps
SF-86 form personal data, security clearance information, fingerprint data, military profiles
Ethnicity, race
Physical attributes, fitness level
Personal descriptions, personal interests
Social connections
Spoken languages
Astrological sign
Political views
Relationship statuses, marital statuses
Family structure, family members' names
Children's names, photos and voice recordings, parenting plans
Religion
Sexual orientations, sexual fetishes
Non-consent sexual videos
Avatars
Beauty ratings

PERSONAL DATA, CONT'D
Car ownership statuses, vehicle details, VINs
Deceased date
Utility bills
Device usage tracking data
Disability ratings
Survey results

BUSINESS DATA
Customer feedback
Financial transactions
Geographic locations
Customer interactions
MAC addresses
Employee names and VPN keys
Authentication tokens, knowledge-based authentication data
Source code
Support tickets
Intellectual property
Intelligence files
W-2 (tax) info of employees, employee ID number, wage and tax information

This list of data breached in these cases is everything a cyber-thief would need to know about someone to answer the "secret forgot password questions" (if they don't already have the answer) and steal identities, blackmail someone, target to sway opinions or purchases, or get into a corporation with either stolen identities, or enough information to impersonate an employee.

TROUBLING TIDBITS

Out of the 433 cases analyzed, there were some troubling tidbits that are indicative of broader trends that are worth calling out:

- **We identified 42 cases where the company had no idea they were breached for years, or they found out from a third-party disclosure.**
  In eight cases, the average time to discovery was 3.2 years. Third-party disclosures of breaches due to datasets being offered on the darknet is very prevalent. In the case of MySpace, they found out about their 360 million-record breach when the records were being sold online. Another continual source of breach notifications are researchers who monitor the darknet for stolen datasets. Researchers publish the lists of companies that have been breached and what data was taken, on "check if you've been breached" sites to warn consumers. In the course of this community service, they often get datasets that have been previously undisclosed.

- **When attackers use stolen data varies greatly.**
  Four days after the breach was the fastest time to resale we found; eight years later was the longest. Some attackers might need the money right away while longer term, strategic threat actors might not be collecting data for the money but rather for intel that's part of a bigger plan.

- **There's so much stolen credit card data, the records aren't worth what they used to be.**
  In one case, 27 million US credit cards were stolen, and sold for only $8,000, or $0.0003 a record.

- **People reuse online credentials, making the attacker reward one-to-many.**
  The Yahoo and Sony hacked databases were joined and de-duped. Fifty-nine percent of accounts had the same username and passwords in both services.

- **One point-of-sale (POS) software, many more customers.**
  The BlackPOS malware was the common thread between Target, Home Depot, PF Chang's, and Sally's Beauty Supply. Because POS systems see the entire card, they can collect enough data to create counterfeit cards, as they did in the case of American Thrift Stores.

- **Passwords are public.**
  We did not find a single case in which passwords were properly hashed. This is likely due to the fact that properly hashing (strong algorithm with a cryptographic salt) or encrypting a dataset that is called upon frequently is very taxing on system processing and can cause login latency. Proper encryption has proven too slow for the request volume. It also requires the application to drop obsolete, broken algorithms and re-encrypt with modern ones.

- **Automated verification systems are easily bypassed with stolen data.**
  Thieves have so much data on people that they can abuse the automated verification systems that require things like SSN, date of birth, or the cards expiration date. In the case of Home Depot,[14] the attackers used the automated verification systems at banks to reset the PINs on the credit cards they

[10] https://myspace.com/pages/blog

[11] http://www.troyhunt.com/2012/07/what-do-sony-and-yahoo-have-in-common.html

[12] https://www.bankinfosecurity.com/home-depot-breach-linked-to-targets-a-7293

[13] http://krebsonsecurity.com/2015/10/credit-card-breach-at-americas-thrift-stores/

[14] http://krebsonsecurity.com/2014/09/in-wake-of-confirmed-breach-at-home-depot-banks-see-spike-in-pin-debit-card-fraud/

[15] https://www.cbsnews.com/news/irs-identity-theft-online-hackers-social-security-number-get-transcript/

[16] https://www.americanbanker.com/news/spike-in-fake-id-schemes-confounds-banks-fraud-filters

[17] https://theintercept.com/document/2014/03/20/hunt-sys-admins/ (published Snowden files)

[18] https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

[19] https://krebsonsecurity.com/2017/05/breach-at-sabre-corp-s-hospitality-unit/

[20] https://www.seattletimes.com/seattle-news/health/data-breach-exposes-info-for-400000-community-health-plan-members/

[21] https://www.justice.gov/usao-sdny/file/632156/download

[22] https://www.justice.gov/usao-ndga/us-vs-viet-quoc-nguyen-and-giang-hoang-vudavid-manuel-santos-da-silva

[23] http://www.reuters.com/article/us-cybersecurity-banks/cybercrime-ring-steals-up-to-1-billion-from-banks-kaspersky-idUSKBN0LJ02E20150215

[24] https://www.cyberwarnews.info/2016/11/08/alaskan-elections-website-hacked-by-cyberzeist-2/

[25] https://www.documentcloud.org/documents/3766950-NSA-Report-on-Russia-Spearphishing.html#document/p1

[26] https://www.equifaxsecurity2017.com/2017/09/15/equifax-releases-details-cybersecurity-incident-announces-personnel-changes/

[27] https://www.csoonline.com/article/2134444/security-leadership/target-cio-resigns-following-breach.html

had stolen. In the case of the IRS, hackers used personal information gathered from other online sources (like bank accounts) to answer personal identity questions on the "Get Transcript" forms.[15]

- **Synthetic IDs—a.k.a. "virtual people"—are on the rise, thanks to the vast quantities and robustness of the breached dataset at the hands of attackers.[16]**

- **Spy agencies target system administrators with phishing attacks powered by social media data.[17]**
This is because they know one admin account can give them the master key to the entire system. This is a known, common technique with international intelligence agencies.

- **It's not just you, it's your vendors.**
Did you even know they existed? Enterprises are getting stunned by attacks coming through seemingly innocuous third parties. Here are just a few cases:

  - Target was breached through their HVAC vendor.[18]

  - Sabre reservation systems used by hospitality and travel sites[19]

  - NTT Data Hosting and the Community Health Plan of Washington[20]

- **A small few can do a significant amount of damage.**
  - Three guys made hundreds of millions of dollars by phishing into major financial institutions, collecting their user databases and spamming their users with pump-and-dump stock schemes.[21]

  - It took authorities 10 years to investigate, arrest, and prosecute these perpetrators.

  - Two guys collected billions of accounts from US email service providers. They then used those accounts to make millions of dollars off of spam and phishing campaigns.[22]

  - Carbanak, a Russian cybercrime gang, stole $1 billion directly from banks. They started by targeting specific employees with spear-phishing campaigns to get access to the administration accounts on the video surveillance system. From there, they watched bank tellers to profile their behavior that they later mimicked when fraudulently transferring money.[23]

- **Trusting election results is legitimately up for debate.**
Hackers claim they had root access to Alaska's voting results server,[24] and US intelligence agencies all agree that Russia interfered in the 2016 US presidential election.[25]

- **Executives, not just the CISO, lose their jobs over major breaches.**
  - Equifax's CSO and CIO "retired" in the wake of the largest credit bureau breach in history, which has (so far) impacted 145.5 million Americans.[26]

  - Target's CIO and CEO both resigned in the wake of the retailer's breach.[27]

- JP Morgan's CSO was pushed out, and the CISO was moved to another division a year after the breach amid criticism on how the breach was handled.[28]

- **Leaked US intelligence agency materials wreaked havoc, and this could be our new norm.**

In April of 2017, a hacker collective known as the Shadow Brokers—a sworn enemy of the NSA offensive cyber team the Equation Group—released an exploit called EternalBlue that targeted Microsoft Server Message Block (SMB). Within a few weeks, it was weaponized into WannaCry, a ransomware worm that spread across Europe and into the US and Asia in early May.[29] It was the inspiration for SambaCry, the Linux-equivalent vulnerability of WannaCry, which targeted Samba, the SMB of Linux. This vulnerability was also released in May.[30] In late June, NotPetya, another ransomware worm leveraging a modified version of EternalBlue, wreaked havoc across Eastern Europe, costing the global shipping giant Maersk $300 million dollars.[31] To make matters worse, the Shadow Brokers have started a monthly subscription service where they release a "wine of the month," including "web browser, routers, handset exploits and tools, select items from newer Ops Disks, including newer exploits for Windows 10, compromised network data from more SWIFT providers and Central banks, and compromised network data from Russian, Chinese, Iranian, or North Korean nukes and missile programs."[32] Perhaps the most troubling aspect of all is that this could be our new norm. Included in the NSA and CIA Vault files are process and procedure blueprints on how the intelligence agencies discover vulnerabilities and create exploits. These can be used by attackers to develop a virtual assembly line of zero-day attacks.[33]

- **Cyberattacks that cause physical damage are becoming common.**

Stuxnet, circa 2009, is perhaps the most well-known malware ever created for physical destruction purposes. It's widely credited for delaying Iran's nuclear weapons program and precluding a war by physically dismantling nuclear centrifuges. January 2017 saw the first confirmed cyberattack that took down a power grid in a major city. The power company, UkrEnergo, in Kiev, Ukraine, was hit with a phishing attack that ultimately enabled attackers to overwrite firmware and "brick" (a cyberattack that destroys an electronic device) the substation power breakers. Technicians had to travel to the substations to physically close breakers and restore power. As a result, the city of Kiev lost power for a few hours, but it could have been much worse. There is widespread speculation, directly from the Ukrainian government, that Russia was behind the attacks and was just using the country as a testbed for refining attacks on critical infrastructure that could be used across the world.[34] Power station breakers aren't the only devices that are getting "bricked." Millions of IoT devices were bricked by a vigilante thingbot called Brickerbot in 2016. Brickerbot was designed to rid the world of IoT devices that were actively being targeted to join the DDoS thingbot, Mirai.[35]

28 https://www.scmagazine.
com/jpmorgan-ciso-
reassigned-over-
handling-of-major-breach/
article/532395/

29 https://f5.com/labs/
articles/threat-intelligence/
malware/from-nsa-
exploit-to-widespread-
ransomware-wannacry-is-
on-the-loose-26847

30 https://f5.com/labs/articles/
threat-intelligence/cyber-
security/sambacry-the-
linux-sequel-to-wannacry

31 https://www.theregister.
co.uk/2017/08/16/notpetya_
ransomware_attack_cost_
us_300m_says_shipping_
giant_maersk/

32 https://steemit.com/
shadowbrokers/@
theshadowbrokers/oh-
lordy-comey-wanna-cry-
edition

33 https://f5.com/labs/
articles/threat-intelligence/
cyber-security/nsa-cia-
leaks-provide-a-roadmap-
to-stealthier-faster-more-
powerful-malware-like-
sambacry-and-notpetya

34 https://www.wired.com/
story/russian-hackers-
attack-ukraine/

35 https://f5.com/labs/articles/
threat-intelligence/ddos/
the-hunt-for-iot-the-rise-of-
thingbots

CONCLUSION

Cyber attackers are like villains in movies, spying on their prey and laughing that evil, "this-is-too-easy" laugh. They continue to get away with their attacks because, in general, security hasn't improved. Organizations still get compromised by the same old tricks, the same old vulnerabilities. Of course, there are outliers. Some organizations do all the right things and haven't been hacked. They are the ones that have to worry about advanced persistent threat (APT) actors targeting and exploiting them. But, for the most part, attackers don't have to engage in advanced reconnaissance activities—casing their targets for months if not years, finding zero-day vulnerabilities and designing new exploits—because too many companies leave their apps and databases wide open for exploit. Even when they don't, too many users are willing and eager to give up their usernames and passwords in social engineering exploits, and the chances are low that the proper mitigating controls are in place.

The rise of social networks has given attackers enormous amounts of data to make their social engineering attacks more powerful. They know where people live, where they work, their job titles and levels, their interests, family structure, and more. The same data that marketers use to target advertising is also used by attackers to sharpen their social engineering attacks. And if there's one thing cyber attackers do better than anyone else in the world, it's share with each other. They share data, tools, automation scripts, exploits, attack plans and techniques, and success stories. Collectively, they work more efficiently and smarter than enterprises do. Globally, enterprises don't share. We don't disclose our incidents or share the details that could help other companies quickly learn how an attack happened, what to look for in logs, what files were injected, and what worked to successfully stop the attack. These are the incident response details that could put other victims a couple steps ahead the next time an attack occurs. Because we don't share enough important information among our peers, reports like this one are necessary.

But, the future of security is not all gloom and doom. We've learned important lessons that become prescriptions for action. Maybe you already knew a lot of the findings in this report but just didn't have the data to prove it. If so, use this report as a tool to jump objectives up the priority ladder. The other good news is that effective solutions exist to thwart 86% of attacks. They do, however, need to be implemented properly, which is difficult and takes time, hence the magnitude of breaches. So, focus on getting the following areas to a state of maturity that will let you sleep at night:

APPS ARE THE NUMBER ONE TARGET, SO SHIFT YOUR FOCUS TO THE TARGETS, AND SECURE YOUR APPS!

- Do you know of all your web application vulnerabilities? Are you sure about that? Are you doing static and dynamic scanning? Does it cover that pesky forum software that's been so heavily modified that it can't take auto-updates anymore? Are your developers fixing the vulnerabilities you find? Better yet, are vulnerabilities being found in QA and fixed before they get pushed to production?

While you're figuring out all of that, implement a web application firewall (WAF). By its nature, it blocks web application vulnerabilities that you don't know about. Just don't 'tune' the policy (a.k.a. poke holes) in a way that opens up the app to exploit, effectively defeating the WAF's purpose. (If you did do this and were breached, search the POST data in the WAF logs to figure out "how" the attackers exploited your app.) Configuring a WAF isn't a remotely easy task to accomplish. It requires security engineers who are proficient in web applications and can properly manage the configuration. They should have good relationships with the application developers who truly know how the applications work. Given how difficult it is to find people with these skills, this is a good control to outsource to a managed service provider. The service provider has a vested interest in the security posture being adequate— and application developers will be more amicable with them.

- How many more Equifax-type breaches need to happen before organizations implement robust patching systems and processes? You need to know about all the systems in your environment; have a solution in place to automate testing and deployment (so days of downtime coordination and system engineering resources aren't required to patch production), and have scanning tools in place to test your patch processes and ensure you don't miss anything.

WE LIVE IN AN ASSUMED BREACH WORLD, SO GET YOUR VISIBILITY IN ORDER.

- Ensure you are aware of all your assets, including third-party connections and hosted environments (sorry—you can't just scan your subnets anymore). Implement controls that give you visibility into attacks that may be happening in your network or systems, including proper logging, and properly tuned intrusion detection and security event monitoring systems. Visibility includes having a traffic decryption device to ensure you aren't passing encrypted—invisible—traffic to your inspection systems. But, it's not enough to just have these systems in place; they need to be properly tuned, otherwise they do nothing but send out "cry wolf" alerts that are ignored.

PREVENT USERS' MISTAKES FROM RESULTING IN MASSIVE DATA EXTRACTION BY USING PROPER ACCESS CONTROL AND ENDPOINT INSPECTION.

You can't trust or control users; because they are easy to exploit, they are your weakest link.

- For phishing cases that send users to fake websites to collect usernames and passwords (to be used later from another system), implement multi-factor authentication (MFA). MFA will catch the new login request from a different IP address and system, and require enhanced verification. Consider MFA mandatory gap assurance.

  - Filtering access to known phishing web sites is also important to do.

- For customer-facing apps that don't support MFA, implement credential stuffing controls that don't allow customers to create accounts with known stolen credentials.

• For phishing cases that rely on users opening a malicious file (which can then exploit a vulnerability on the system), patch, update, and patch again! If you don't do this, your systems will be pwnd. At a minimum, all endpoints should have:

  - The latest operating system patches applied within a week of release

  - Current bowsers (do not fall behind the two latest versions)

  - The latest Flash and Java updates (this is very important!)

  - Continually updated anti-virus software (do not allow this to be overwritten!)

• Limit the number of username and passwords that users need to create and manage by implementing both single sign-on and federated identity. Single sign-on is only a partial solution. Users still have to keep entering that username and password everywhere, but if you give them federated identity, it will securely log them onto all the applications they need (provided it's set up) without having to enter their credentials over and over again. Users will love you for this (and you'll need a win after forcing them through all the hoops).

• Users with high levels of network access, and access to high valued assets, must be properly and continually trained. If intelligence agencies hunt system administrators, attackers do the same. If attackers know who works in HR and Accounting because they trolled them on LinkedIn, those people will be sent spear-phishing attacks.

Keep in mind, once organizations improve security around the main ways attackers get in now, attackers will revert to using other attacks in other areas of the network that were neglected while you were securing your apps and implementing access control systems. So, it's essential to keep doing what you've been doing in those areas.

APPENDIX A: SOURCES

Content from the following sites was used to collect case data for this research report.

Note: The full raw dataset used to calculate these results is not being made public in this report. Readers who are interested in the underlying calculations may send a request to f5labs@f5.com.

000webhost.com	darkreading.com	kaspersky.com	reuters.com
atr.org	ebayinc.com	krebsonsecurity.com	riskbasedsecurity.com
bbc.com	economictimes.indiatimes.	law.com	sec.gov
blog.avast.com	com	leakedsource.ru	securelist.com
bloomberg.com	epic.org	mass.gov	symantec.com
breachlevelindex.com	eweek.com	money.cnn.com	techarp.com
businessinsider.com	fortune.com	motherboard.vice.com	thehackernews.com
calgaryherald.com	haveibeenpwned.com	nakedsecurity.sophos.	theregister.co.uk
cbsnews.com	huffingtonpost.com	com	tripwire.com
cnet.com	ibtimes.co.uk	nbcnews.com	wholefoodsmarket.
cnn.com	independent.co.uk	nytimes.com	com
computerworld.com	informationisbeautiful.net	oag.ca.gov	wired.com
csoonline.com	investorplace.com	ocrportal.hhs.gov	wsj.com
cyberwarnews.info	jpost.com	redlock.io	zdnet.com

F5 LABS

APPLICATION THREAT INTELLIGENCE

f5