Data Breach Industry Forecast **2019**

By Experian® Data Breach Resolution

Executive Summary

While it's been about 13 years since one of the first major data breaches reverberated on the nation's radar, there is still no slowing down—despite major security advancements—in the amount of incidents and consumers impacted every year.

The scale of some of the data breaches in 2018 have been staggering and the number of records compromised in the first half of the year had already surpassed the total number of breached records for all of 2017, according to the Identity Theft Resource Center's 2017 Data Breach Industry Summary report.

It's safe to say that hackers are not necessarily catching organizations off-guard, data breach preparedness is at an all-time high, according to our annual study with the Ponemon Institute, with 82% of companies saying they have a response plan in place. However, cybercriminals are increasingly becoming more sophisticated and it's a constant game of cat and mouse.

In our sixth annual edition of this Data Breach Industry Forecast, we investigated some new breach frontiers that hackers can exploit like biometrics, but also address the basics, so to speak, looking at breach surfaces such as the Cloud that present vulnerabilities that haven't been tapped out just yet.

Experian Data Breach Resolution outlines five predictions for the data breach industry in 2019. We've also added a bonus prediction, by Experian's dark web expert, as breaches and the dark web are intertwined today with consumers' information being exposed in a data breach ultimately ending up on the dark web for sale. We also look back on our predictions for 2018. Our predictions are rooted in Experian's history of helping companies navigate more than 25,000 breaches over the last decade.

Based on our experience, the top data breach trends of 2018 include the following:

» Attackers will zero in on biometric hacking and expose vulnerabilities in touch ID sensors, facial recognition and passcodes.

» Skimming isn't new but the next frontier is an enterprise-wide attack on a national network of a major financial institution, which can cause millions in losses.

» A major wireless carrier will be attacked with a simultaneous effect on both iPhones and Android, stealing personal information from millions of consumers and possibly disabling all wireless communications in the United States.

» It's only a matter of when, not if, a top cloud vendor will suffer a breach, compromising the sensitive information of hundreds of Fortune 1000 companies.

» Friends or foes? The online gaming community will be an emerging hacker surface, with cybercriminals posing as gamers and gaining access to the computers and personal data of trusting players.

#1 BIOMETRICS

Biometrics are an increasingly popular form of authentication. While biometric solutions offer a security layer for data, biometric data will gain value to cybercriminals and is at risk for theft and fraud.

PREDICTION

Attackers will zero in on biometric hacking and expose vulnerabilities in touch ID sensors, facial recognition and passcodes.

Organizations are embracing biometrics to address their cybersecurity concerns. The majority of IT professionals believe biometrics is the most secure method of authentication available right now, and company leadership is buying in, with 63 percent[1] having either implemented or planning to onboard a biometric system. Passwords are no longer effective at protecting data, and as organizations must now work within parameters dictated by the General Data Protection Regulation and other privacy regulations, turning to biometrics as part of a multi-factor or stand-alone option appears to be the best approach. In addition, an increasing number of personal devices like smartphones and tablets have biometric options.

However, biometric authentication isn't foolproof. Shortly after Apple introduced fingerprint authentication on the iPhone, hackers showed how easy it is to steal a fingerprint and use it to gain access to a device.

Biometric hacks also involve potential incidents of fraud. We've already seen the theft of biometric data. The Office of Personnel Management breach included the theft of more than five million unencrypted fingerprints. As use of biometric authentication grows, so does the risk of biometrics becoming a target and a tool for cybercriminals.

Sensors can be manipulated and spoofed or deteriorate with too much use. Biometric data, also, can be altered when it is first recorded. Expect hackers to take advantage not only of the flaws found in biometric authentication hardware and devices, but also of the collection and storage of data. It is only a matter of time until a large-scale attack involves biometrics either by hacking into a biometric system to gain access or by spoofing biometric data. Healthcare, government, and financial industries are most at risk.

The Takeaway:

Organizations need to ensure their biometric systems are secure in all layers. Biometric data should be encrypted and stored in secure servers. Privacy regulations may come into play in how biometric data is treated in the future, although now it is fairly unregulated. Until sensors, scanners, and other hardware are better able to detect anomalies, biometrics should be used as part of a multi-factor authentication system.

Card skimming remains a serious identity theft risk, but cybercriminals have added a digital layer. Now they are able to skim thousands of credit cards from ecommerce sites with a simple and virtually undetectable malware download.

#2 SKIMMING

PREDICTION

Skimming isn't new, but the next frontier is an enterprise-wide attack on a major financial institution's national network, which could result in millions in losses.

Anyone who uses a credit card at a gas pump or an ATM is—or should be—aware of card skimmers, which are hidden devices designed to steal card information and passcodes. It's an attack technique that has been in play for a long time, yet it remains one of the most common and most successful trends for data breaches today.

ATM skimming is such a problem in Southeast Asia that travelers are warned about the risks of identity theft as well as potential financial loss if they try to access the machines while on vacation. It is a problem that is on the upswing across the United States. However, criminals aren't just physically targeting ATMs, but now going after bank networks. By either directly loading malware into the ATM or using social engineering tactics to download malware into the computer system, criminals can infect the network that operates the ATM and empty the bank's safe.

Cybercriminals have also taken skimming digital.

Using skimming malware, a cybercriminal group known as Magecart was able to breach British Airways, Newegg, and Ticketmaster to steal thousands of credit card numbers, as well as other personal and financial information from customers. In both the British Airways and Newegg cases, malware was injected directly into the website, which was then shared with the mobile app. Ticketmaster's breach involved a third-party site.

The cybercriminals can avoid detection because they were able to blend into the organization's infrastructure. This allows them to do a lot of damage before there is any sign of a problem. Using malware to skim financial and personal information is still in its early stages and cybercriminals are just beginning to see the value in this type of attack. Right now there are few criminal players in the game, but expect malware-based skimming to continue to evolve.

The Takeaway:

Don't get blasé about old school attacks. Skimming hasn't reached its pinnacle yet. And because cybercriminals are using proprietary web technology and network infrastructure, it is very difficult to detect an attack until it's too late. Organizations should monitor their networks for anomalies to financial transactions, especially when there are no other customer transactions involved.

Wireless systems are vulnerable. A single attack on a major wireless carrier could disrupt communications, creating chaos.

#3 WIRELESS CARRIER MAJOR ATTACK

PREDICTION

A major wireless carrier will be attacked with a simultaneous effect on both iPhones and Android, stealing personal information from millions of consumers and possibly disabling all wireless communications in the United States.

The information on your smartphone may be more valuable than anything on a more traditional computer. Your smartphone reveals your location, your list of contacts, photographs, your interests, financial information – the list is endless. All of this information is why hackers want access to your phone. It will tell them everything.

In fact, earlier this year the Department of Homeland Security issued a warning to Americans that "nefarious actors" were tapping into locations of cellphone users and their calls as well as texts to use information against Americans as they travel globally.

A CBC news investigation even showed how easy it was for hackers to gain access to a phone through the wireless carrier. The attack penetrated Signalling System No. 7 (SS7), a layering system that allows for phone, data, and billing connections. The investigation was able to track an individual phone's location and access the contents just by having the phone number.

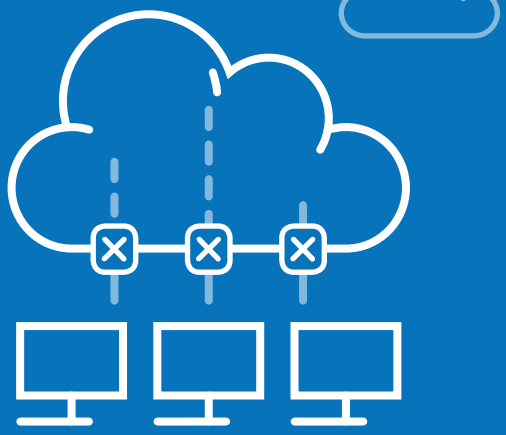
These incidents show that the wireless environment is vulnerable. Because we are so dependent on our phones, tablets and other connected devices, a serious disruption to wireless service could wreak havoc on society. Let's face it – sometimes attackers just look to cause wide-scale chaos and, similar to infrastructure, focusing on the wireless environment would halt the nation. It could effectively shut down communication across the country, harming business operations and putting emergency services at risk. Individual phones could also be targeted in a wireless carrier attack through malicious queries searching to gain unauthorized access.

The Takeaway:

Because smartphones are so integral to every aspect of society, both phone manufacturers and wireless carriers need to work together to fix the flaws in SS7 and make it more difficult to track phones just by a phone number.

Cybersecurity professionals already worry about data security in cloud computing environments at the organization level, but an attack at the vendor level will affect hundreds of companies at once.

#4 CLOUD



PREDICTION

It's only a matter of *when*, not *if*, a top cloud vendor will suffer a breach, compromising the sensitive information of major companies.

Security has always been a concern in cloud computing. Among those in charge of cybersecurity, nine out of ten cybersecurity professionals say it's very worrisome, according to the 2018 Cloud Security Report by Cybersecurity Insiders. This has increased since last year's survey. The report cited that the top three cloud security challenges include protecting against data loss and leakage, threats to data privacy, and breaches of confidentiality.

As more companies are adopting cloud computing systems, reports show that monitoring for potential threats is low.

This opens a door for cybercriminals to take advantage of the vulnerabilities in the cloud. Uber, Time Warner Cable, and Accenture were large enterprises hit with a data breach because of a misconfiguration in Amazon Web Services cloud, for example. While the fault was on the subscriber end, it raises questions about overall security on the vendor side and how long it will take hackers to skip the middleman and go straight to the cloud source, which would affect the world's largest companies and potentially billions of pieces of data.

The Takeaway:

Cloud security is improving, but cloud misconfiguration raises new concerns about security at all layers. Improved monitoring systems should be in place to alert for misconfiguration and vulnerabilities. There needs to be a well-defined hierarchy of responsibility and liability for security and monitoring, and accountability for when something does go wrong. We'll probably see more private cloud hosting over the public cloud in the future as a result.

#5 GAMING

Online gaming presents a new and varied attack vector for cybercriminals.

PREDICTION

Friends or foes? The online gaming community will be an emerging hacker surface, with cybercriminals posing as gamers and gaining access to the computers and personal data of trusting players.

The Sony Playstation breach in 2011 was an early indication that gamers had information of value to hackers. Almost a decade later, the rising popularity of eSports has turned it into a $1.5 billion industry. Approximately a quarter of the world's population, or 2.2 billion people, are gamers[2]. Many of these gamers use cryptocurrency, or want greater opportunities to use it, to build more competition on a global scale.

All of these gamers, and adding in cryptocurrency concerns, creates a serious cybersecurity challenge.

Gamers are known for their anonymity. Even the most famous gamers are known only by their online names and personas. This means cybercriminals can easily pose as a gamer, build trust within a particular game or community, and gain access to privileged inside information. It isn't just the personal PII or credit cards that are of value in the gaming world; there are the tokens, weapons, and other game pieces that are worth a lot of money within a gaming community. With a single password—and gamers tend to practice poor password protections—a hacker can take over someone else's avatar and identity within a game without detection and walk away wealthy.

It isn't just theft that is a concern. Cybercriminals are going into the gaming world to cause chaos. A popular children's video game, Roblox, was infiltrated by bad actors who simulated a rape of a little girl's avatar while the girl was playing the game. The hackers went around the system's protections to customize animations. Female gamers have long been harassed and threatened, a situation that will get worse as more people enter an unregulated gaming world.

The Takeaway:

The onus is on the gaming world to beef up security at all levels. Gamers are of all ages, but many are younger players who don't understand security practices or don't see the need because they believe it is a trusted community. Cybersecurity should be baked into the hardware and networks, with stronger authentications to make it tougher for others to take over characters. Some regulation and oversight are necessary to strip away the total anonymity of players.

Trend to Watch:

Hackers will begin to use more multi-vector attacks against your broader digital identity.

By Brian Stack
Vice President of Dark Web Intelligence
Experian

Between 2005 and 2017, significant data breaches—the type that affected millions of users—rose from about 200 per year to more than 1300. Billions of pieces of data are exposed and easy for cybercriminals to monetize. This has led to a rising risk of identity theft. Protecting consumer data and organizational network infrastructures from potential cyber threats is a day-in and day-out battle. But, the time has come for consumers to step up and take control of their digital identity.

Most attacks against consumers are targeted on a single vector—exposure of data. This happens through different means, such as phishing email, SSNs exposed during a breach, malware installed from malicious websites and so on. While this is a stressful situation for consumers, security teams do have the tools and systems in place to mitigate these types of attacks.

However, because of the unprecedented amount of personal data available, coupled with the commoditization and ease of access of hacking tools and services, expect cybercriminals to change tactics and focus on multi-vector attacks. Hackers still want to steal all that data, but now they want to turn your devices into botnets that can cause even more damage.

It's a low risk, high yield proposition for cybercriminals, as botnet pay-per-installation services can be bought on the Dark Web at minimal costs. This means that the cyber attack of tomorrow will still include attack methods to steal SSNs and other identifying personal information, but will also include hijacked cell phones and internet services. Multi-factor authentication methods that rely on text messages, phone calls, or email will send pin codes to someone else who now has that access.

The Takeaway:

In the future, consumers' will need a comprehensive plan and monitoring in place to protect their larger digital identity. Consumers must be prepared to regain control if they are victims of a multi-vector attack. The ability to respond quickly will be critical in ensuring financial assets are secure and protecting from ongoing or future attacks against their digital identity.

2017 Forecast Scorecard Ratings

Failure to comply with new European Union regulations will result in large penalties for U.S. companies

A

Update: Google and its parent company Alphabet was fined $5 billion for violating EU competition regulations. Facebook's data breach, revealed in September, involved at least three million EU users, but because the company complied with the 72-hour reporting requirement, that could play a role in disciplinary action, including fines. The EU could make an example of these giants to other U.S. companies and we will probably see more fines as court verdicts reach their completions.

Vulnerabilities in internet of things (IoT) devices will create mass confusion, leading to new security regulations.

A

Updates: California passed a law, separate from the California Consumer Privacy Act, addressing default passwords in IoT devices and address IoT vulnerabilities. Many experts believe that any cybersecurity laws passed in California will impact the entire country. There will likely be more government and industry groups stepping up next year to enforce regulations on manufacturers.

Perpetrators of cyberattacks will continue to zero in on governments, which could lead to a shift in world power.

B

Update: There have been a number of incidents of individual campaigns that were targeted for spearphishing attacks and DDoS attacks on candidate websites during the 2018 midterm election cycle. There are reports the U.S. Cyber Command warned Russians about interference in elections. Also, warnings have been posted about potential attacks on the 2019 EU elections. Major players on the world stage—China and North Korea—as well as Russia are throwing their weight around when it comes to being the most accomplished nation at state sponsored attacks, which could give them more global leverage. We are seeing a lot of action involving cyberattacks targeting government entities and this won't slow down.

The United States may experience its first large-scale attack on critical infrastructure, causing chaos for governments, companies and private citizens

C

Update: It was reported in July 2018 that Russian hackers targeted hundreds of companies across various critical infrastructure sectors, including electric power utilities and nuclear plants, with several actually being compromised, according to the Department of Homeland Security. In one case, the criminals were able to get access to the controls behind a small power generator but didn't turn the switches. Recently, we learned that data was exposed within the systems of electrical engineering operator, Power Quality Engineering, which allowed any interested browser to download sensitive electrical infrastructure data compiled in reports by PQE inspectors examining customer facilities. While we know systems are under attack, there hasn't been any reports of outages or large-scale events caused by intruders however.

Attackers will use artificial intelligence (AI) to render traditional multifactor authentication methods useless.

C

IBM has found some evidence of AI-based cyberattacks that will target authentication methods like biometrics and geolocation, but we haven't seen any major attacks powered by AI yet. Companies are getting ahead of it and top cybersecurity companies are actually using AI to combat cyber attacks. There is still a way to go for AI to be a bullet for hackers to take down multifactor authentication, but companies shouldn't get complacent here either.

About Experian Data Breach Resolution

Experian Data Breach Resolution, powered by the nation's largest credit bureau, is a leader in helping businesses prepare for a data breach and mitigate consumer risk following breach incidents. With more than a decade of experience, Experian Data Breach Resolution has successfully serviced some of the largest and highest-profile data breaches in history. The group offers swift and effective incident management, notification, call center support, and fraud resolution services while serving millions of affected consumers with proven credit and identity theft protection products. Experian Data Breach Resolution is active with the International Association of Privacy Professionals, NetDiligence, Advisen, the Ponemon Institute RIM Council, and is a founding member of the Medical Identity Fraud Alliance.

For more information, visit Experian.com/DataBreach and follow us on Twitter @Experian_DBR.

Footnotes

1. Veridium study 2018
2. https://hackernoon.com/the-inevitable-next-step-for-esports-73e6ed3f5d54