FOURTH ANNUAL 2017

DATA BREACH INDUSTRY FORECAST

By Experian® Data Breach Resolution

EXECUTIVE SUMMARY

Today's world of data breaches is one that is constantly changing. As companies are better prepared to protect against a data breach, attackers are finding more stealthy ways to get around security measures and seek the information they want. While some tried and true attacks continue to serve as go-to methods for hackers, there are evolving tools and targets that are likely to become front page news in 2017. Organizations can't wait until an attack happens to ensure they are protected – they need to look at the signs early on to start preparing for new types of security threats.

A recent study from the Ponemon Institute shows that while more organizations have put data breach response plans into place, a level of complacency has set in with many companies that is preventing them from being fully ready to respond to the types of attacks they are most likely to face.[1] Many are lagging in practicing and updating their response plans as well as keeping up with new types of attacks.

As companies look to 2017, Experian® Data Breach Resolution has outlined five predictions for the data breach industry in the new year. As our fourth annual edition, this data breach industry forecast report hopes to shed light on emerging trends companies should know about and prepare for. The industry predictions included here are rooted in Experian's history helping companies navigate more than 17,000 breaches over the last decade.

Based on our experience, the top data breach trends of 2017 are anticipated to include the following:

» Aftershock password breaches will expedite the death of the password

» Nation-State cyber-attacks will move from espionage to war

» Healthcare organizations will be the most targeted sector with new, sophisticated attacks emerging

» Criminals will focus on payment-based attacks despite the EMV shift taking place over a year ago

» International data breaches will cause big headaches for multinational companies

FOLLOWING THE 2012 AND 2014 BREACHES OF LINKEDIN, DROPBOX AND YAHOO ACCOUNTS, THOSE PERSONAL ACCOUNT DETAILS RESURFACED ON THE DARK WEB IN 2016, RE-EXPOSING 732,000,000 EMAIL ADDRESSES AND PASSWORDS.[2]

1 AFTERSHOCK PASSWORD BREACHES WILL EXPEDITE THE DEATH OF THE PASSWORD

A new industry trend emerging this year, in 2017 we predict “aftershock” breaches as companies are facing the impacts of previous data breaches. As more and more personal credentials are compromised, the risk for users may extend far beyond the initial breach as attackers continue to sell old username and password information on the dark web, sometimes years after the credentials were originally stolen.

As a result, companies that didn’t experience a first-hand data breach may see repeat unauthorized log-ins and be forced to notify their users that their information is being misused. This can be compared to an earthquake “aftershock” where the effects of an attack reverberate and are felt long after the initial disaster.

> Unfortunately, the potential damage of an aftershock breach is likely the same as when the primary organization loses personal information. Customers of these businesses are likely to express concerns and the potential for fraud is as tantamount as the original incident.

As we saw in 2016, a breach of 500 million Yahoo accounts in 2014 continued to echo consequences. It has been reported those stolen credentials were subsequently resold and used by other criminals to compromise accounts across a wide variety of services where consumers use the same username and password. This exposure of the largest ever breach of usernames and passwords is likely to reverberate for years to come as the exposed credentials make their way through the underground economy. Companies that have never experienced a direct breach will be forced to deal with the aftershock of Yahoo’s loss of user credentials.

Given the continued success of aftershock breaches involving username and passwords, we predict that attackers are going to take the same approach with other types of attacks involving even more personal information, such as social security numbers or medical information.

The Takeaway:

Due to these ongoing aftershock breaches, more companies should push toward using two-factor authentication to verify users, which helps solve the password reuse problem. Secondary authentication methods could include tokens, SMS alerts, geo location confirmation or bio metrics.

Companies should also account for aftershock breaches in their incident response plans and ensure they treat them just as seriously as a traditional breach. When disclosing the issue, they should provide guidance to customers about how to reset their passwords and educate them about the broader risk associated with password reuse across websites.

THE FBI WARNS THAT 'ADVANCED PERSISTENT THREAT' CYBER ATTACKERS ARE INCREASINGLY TARGETING SENSITIVE INFORMATION STORED ON U.S. COMMERCIAL AND GOVERNMENT NETWORKS THROUGH CYBER ESPIONAGE.[3]

2 NATION-STATE CYBER-ATTACKS WILL MOVE FROM ESPIONAGE TO WAR

Building upon last year's prediction that cyber conflicts between countries are leaving consumers and businesses as collateral damage, we may see a clear evolution of these types of threats moving from espionage to active conflict and possibly war between countries. While the OPM breach of 2015 was clearly motivated by gaining specific intelligence, in 2017 we will see new operations made public that use cyber-attacks as an outright offensive weapon. In 2016, we saw the issue of state-sponsored cyber-attacks come up during the U.S. presidential campaign. Both candidates were questioned about the U.S. potential response to the use of targeted cyber-attacks by foreign nations, and each candidate expressed that they would be in favor of using cyber weapons to retaliate against countries. We believe that cyber warfare attacks against the U.S. will continue in 2017, and with both presidential candidates taking such a strong and pointed position on how to respond, we predict an escalation in cyber-attack conflict in 2017.

> The progression of cyber-attacks driven by nation-states will undoubtedly place critical infrastructure in the crosshairs, potentially leading to widespread outages or exposed personal information that could impact millions of innocent consumers.

As these types of state operations become more conspicuous, attacks may escalate to the point where countries will be forced to explain them to their citizens. It may also lead to targeted countries retaliating with sanctions or even cyber-attacks of their own. Unfortunately, until there is a clear international agreement regarding rules of engagement in cyberspace, these attacks are likely only going to increase and escalate.

Given the volatile cyber-conflict landscape, we predict that the United States will disclose at least one major offensive cyber operation against a terrorist organization like ISIS or in retaliation for an attack by another nation-state.

Further, it will be essential that companies participate in their respective Information Sharing and Analysis Center to share information about cyber threats among their peers and with national defense organizations.

The Takeaway:

As countries organize targeted cyberattacks, businesses should prepare for full-on disruption, particularly if they are a part of critical infrastructure. Organizations will need to stay vigilant about their potentially exposed information and take proactive steps to protect themselves, including purchasing proper insurance protection and shoring up their security measures to protect against large-scale disruptions.

> **"ONE OF THE BIGGEST CURRENT THREATS TO HEALTH INFORMATION PRIVACY IS THE SERIOUS COMPROMISE OF THE INTEGRITY AND AVAILABILITY OF DATA CAUSED BY MALICIOUS CYBERATTACKS ON ELECTRONIC HEALTH INFORMATION SYSTEMS, SUCH AS THROUGH RANSOMWARE."[4]**
>
> ~ **Jocelyn Samuels**
> Director of The HHS Office For Civil Rights

3 HEALTHCARE ORGANIZATIONS WILL BE THE MOST TARGETED SECTOR WITH NEW, SOPHISTICATED ATTACKS EMERGING

The healthcare sector may continue to be the focal point for hackers as medical identity theft remains lucrative and easy for cyber criminals to exploit. Personal medical information remains one of the most valuable types of data for attackers to steal, and cyber criminals will continue to find a market for reselling this type of sensitive information on the dark web. According to a report from IBM[5], more than 100 million healthcare records were compromised, making them a hacker's top target. We also anticipate mega breaches will move on from focusing on healthcare insurers, which served as a popular attack victim in 2015, to focus on other aspects of healthcare, including hospital networks. These more distributed networks present a ripe target for attackers as it is often harder to maintain security measures as compared to more centralized organizations.

Of the potential sources for a breach, electronic health records (EHR) are likely to be a primary target for attackers. The portable nature of this information and the number of different entities and end-points that need access to them mean the potential for them to touch a vulnerable computer system is high. While there may be significant protections in place to secure them in transit, it only takes one compromised or outdated system to lead to exposure. Further, as more healthcare institutions deploy new mobile applications, it's possible that they will introduce new vulnerabilities that will also be attractive targets for attackers.

Focus on Ransomware: Of the many threats healthcare organizations face, we predict that ransomware will continue to be a top concern in 2017, particularly because a disruption of healthcare system operations could be catastrophic. Ransomware presents an easier and safer way for hackers to cash out; given the potential disruption to a company, most organizations will opt to simply pay the ransom. This has unintended consequences of funding more research and development by attackers who will in turn develop more sophisticated and targeted attacks. These new variants will likely be able to evade many of the security detection systems that were developed and are now widely deployed to stop the previous generation of attacks.

Ransomware attacks may also move from just locking systems to outright stealing information to either sell or leverage for identity theft. Additionally, with the recent Office of Civil Rights (OCR) guidance classifying ransomware attacks as requiring consumer notification, we are likely to hear about a larger number of these types of cases when compared to other sectors.

The Takeaway:

As attackers shift their focus, an increase in hospital breaches means the consequences for healthcare organizations that don't properly manage this risk will increase. Healthcare organizations of all sizes and types need to ensure they have proper, up to date security measures in place, including contingency planning for how to respond to a ransomware attack and adequate employee training about the importance of security.

ACCORDING TO AN INDUSTRY STUDY FROM EARLIER THIS YEAR, ONLY 37 PERCENT OF RETAILERS IN THE UNITED STATES CAN PROCESS CHIP CARDS.[6]

4 CRIMINALS WILL FOCUS ON PAYMENT-BASED ATTACKS DESPITE THE EMV SHIFT TAKING PLACE OVER A YEAR AGO

In 2016, we predicted that the EMV Chip and PIN liability shift would not put an end to payment breaches, and unfortunately, we believe this trend will only continue into 2017. Driven by uneven adoption of the new technology, combined with attackers targeting new industries and adapting their tactics, we predict that payment attacks will continue to vex companies in the year to come.

> Instead of targeting big name retailers as we've seen in the past, attackers may turn their attention to smaller franchised stores and others with distributed infrastructure. Along with needing to manage more distributed infrastructure, these businesses are experiencing other barriers such as the need for software updates to accept payments that are not available and the impact it can have on the checkout process.

The Skim Is In: Attackers are also going to use new techniques in mass to steal payment cards through well-coordinated and expansive use of different types of Point-of-Sale (POS) skimmers. While this technique has been used on a smaller scale by cybercriminals for years, it's likely to grow, especially in the retail sector as self-checkout terminals become more popular.

These skimmers are capable of stealing magnetic stripe data from POS systems even after they've been hardened against more traditional malware-based attacks. We are likely to see criminal gangs develop coordinated and widespread skimming operations to ensure the steady flow of payment cards continue to make a significant profit. We predict that at least one major national retailer will be hit with a significant skimming outbreak over the next year.

The Takeaway:

Payment related breaches will continue to make headlines in 2017, as merchants are still vulnerable to attack as the EMV Chip and PIN transition slowly continues. While there certainly are legitimate barriers for some businesses to adopt the technology, the risk of not doing so is too high to ignore. It is essential that companies behind the curve speed up their plans for EMV Chip and PIN adoption. Both retail companies and consumers need to maintain security best practices during this time of ongoing transition and recognize that cyber criminals may shift their focus but won't be completely deterred. Paying close attention to potential weak spots, including catching POS skimmers quickly, can help mitigate potential fallout.

WHEN THE GDPR REGULATIONS GO INTO EFFECT, ANY COMPANY THAT HANDLES EU CITIZENS' DATA MUST REPORT DATA BREACHES WITHIN 72 HOURS.[7]

5 INTERNATIONAL DATA BREACHES WILL CAUSE BIG HEADACHES FOR MULTINATIONAL COMPANIES

Of the breaches making headlines in 2017, we predict the ones that will cause the most significant damage will involve the loss of international consumers' data. In particular, the General Data Protection Regulation (GDPR) in the EU will create more pressure for businesses and greater consumer awareness around breach notification. Similarly, new regulations set to take effect in Canada[8] and a data breach bill in Australia[9] will likely cause companies to reevaluate their incident response plans and notification standards in those regions as well.

These breaches are likely to have a disproportionately high impact on companies. As many international consumers are not accustomed to being notified of a breach, they are likely to be much more vocal in their concern and will be more likely to stop doing business with a company as a result of an incident.

Further complicating matters, many companies are struggling to prepare for managing a breach involving international populations. According to a recent study from the Ponemon Institute, 42 percent of companies have not included processes to manage an international data breach in their incident response plans[10].

Given the high-stakes in an international breach and the lack of preparedness, we expect that at least one United States multinational company will experience a significant loss in its valuation due to an international data breach in 2017.

The Takeaway:

Companies need to start working to comply with the new rules over the next year as scrutiny of their practices and consumer awareness is raised in more markets. Now is the time for these companies to do "dry runs" prior to the new regulations going into place to ensure they are properly prepared.

OTHER TRENDS TO WATCH

VIRTUAL REALITY AND AUGMENTED REALITY: NEW TOOL FOR HACKERS

The growing popularity of virtual and augmented reality is reaching into new industries every day. Similar to the growth of IoT a few years ago, this is a new and exciting space that may be growing so quickly that proper security measures aren't always put into place. Criminals are likely to target these new technologies with attacks that steal personal information.

For example, the wildly popular mobile game Pokémon Go that encourages users to travel to specific destinations to 'capture' Pokémon could be used by criminals to lure players to certain locations to conduct "Man in the Middle" attacks. The bandwidth demands of these types of interactive games cause many users to connect to unsecure Wi-Fi signals in order to 'catch' the Pokémon before they are gone. By setting up rough Wi-Fi hotspots at places where many will look for Pokémon, attackers could attempt to steal any and all data being sent from victims' phones.

Kids in particular who engage in virtual or augmented reality games may be susceptible to falling victim as they are less likely to understand security risks. In 2017, virtual and augmented reality programs will likely continue to become more mainstream, and it's only a matter of time before criminals take advantage of lax security measures to launch a widespread attack.

IRS TAX SCAMS WILL IMPACT THE 2016 TAX SEASON DUE TO EMPLOYEE NEGLIGENCE

Similar to the 2016 W2 phishing attacks, hackers may continue to target companies around tax fraud, in large part due to the lack of action taken by the IRS. Despite a push from the private sector, it appears that the IRS has not taken adequate steps to alert people when a tax form has been filed. Additionally, current defenses appear somewhat arbitrary and not sufficient to combat the risk. Hackers have found that it can be much easier and more lucrative to target and exploit individual victims versus computer systems for monetary gain. While it may take weeks or months to hack a system and discover where valuable information is stored in order to steal it, a few simple well-crafted, targeted emails to unaware employees can lead to gaining the same amount of information with little effort.

These types of scams continue to work because companies are failing to train their employees on identifying phishing attacks. According to a recent study from the Ponemon Institute, less than half (49 percent) of organizations include phishing and social engineering attacks in their employee security trainings.[11] In 2017, more individual employees will be fooled by social engineering tactics, leading to a spike in tax fraud related to employee negligence. On top of tax-related scams, other targeted employee scams will be successful despite warnings from law enforcement about these types of attacks. The most prominent example will likely be schemes that cause members of the finance department to make money transfers to attackers.

PREDICTIONS SCORECARD: RATING OUR 2016 PREDICTIONS

As we do each year, to hold ourselves accountable, we graded how our 2016 predictions panned out. Overall, last year's predictions were fairly accurate, although there were some surprises:

A

THE EMV CHIP AND PIN LIABILITY SHIFT WILL NOT STOP PAYMENT BREACHES

The implementation of EMV Chip and PIN technology, and the liability shift that came along with it, did not stop payment breaches. Recent breaches at restaurants like Wendy's and CiCi's Pizza, and the Oracle MICROS breach show that while EMV may make payments more secure, it will not stop breaches since not all systems are prepared and hackers will continue to look for weak spots in the payment process.

B

BIG HEALTHCARE HACKS WILL MAKE THE HEADLINES, BUT SMALL BREACHES WILL CAUSE THE MOST DAMAGE

In 2016, there were 181 reported healthcare breaches ranging in size from 500 to 3.6 million effected individuals. While several large breaches like Banner Health and 21st Century Oncology lost more than 5 million records combined, small breaches also had a large impact. Breaches impacting 200,000 people or less accounted for 96 percent of all healthcare related breaches and impacted 1,400,872 individuals.

A-

CYBER CONFLICTS BETWEEN COUNTRIES WILL LEAVE CONSUMERS AND BUSINESSES AS COLLATERAL DAMAGE

Cyberattacks between countries have continued in 2016 and have left consumers and businesses exposed. While most countries have used cyberattacks for espionage, Russia (or pro-Russia supporters) showed the power of a well-coordinated cyberattack by knocking out the power to more than 225,000 people. This event took place at the end of 2015, but is only one example of how Russian supporters are using cyberattacks during this armed conflict. Additionally, Chinese attacks against the U.S. government and companies have continued despite Obama and President Xi Jinping's agreement to crack down on intellectual property theft. Initial reports conducted by iSight showed a decline in attacks, but State Departments reports noted that this decline was likely due to covert cyber tools and methods rather than an actual decline in attacks.

A

2016 U.S. PRESIDENTIAL CANDIDATES AND CAMPAIGNS WILL BE ATTRACTIVE HACKING TARGETS

The 2016 presidential race proved to be an attractive target for hackers, as demonstrated by the DNC hack, which released damning emails from top party officials. As the origin of the hack is still unknown, despite suspicions that Russia conducted the hack, one thing is for certain, political campaigns can no longer ignore cybersecurity. The impacts of the DNC hack moved beyond party officials and embarrassing emails, to identity theft of a major donor. The Trump campaign was not immune to attacks either, with hackers taking over his website several times.

C

HACKTIVISM WILL MAKE A COMEBACK

Hacktivisim continued throughout 2016, however, its resurgence was not as prominent as predicted. While hacks against ISIS did receive several pieces of coverage, generally hacktivist efforts have not had the same impact as in years past. Of note, Anonymous continued to target international banks and governments with DDoS attacks.

Experian® Data Breach Resolution
(866) 751-1323
Experian.com/DataBreach
databreachinfo@experian.com
@Experian_DBR

Footnotes:

1. "Fourth Annual Study on Data Breach Preparedness," Ponemon Institute, October 2016
2. "Have I Been Pwned?"
3. "FBI Flash: Vulnerabilities and Post Exploitation IOCs for an Advanced Persistent Threat," May 2016
4. "Ransomware and Health Care: There's More at Risk Than Just Money," SecurityIntelligence, August 2016
5. "2016 Cyber Security Intelligence Index," IBM
6. "EMV Merchant Adoption Slower Than Expected," The Strawhecker Group, February 2016
7. "What does shake-up of EU data laws really mean?" BBC News, April 2016
8. "Digital Privacy Act," Canada Minister of Industry
9. "Serious Data Breach Notification Bill," Australian Attorney-General's Department
10. "Fourth Annual Study on Data Breach Preparedness," Ponemon Institute, October 2016
11. "Managing Insider Risk through Training & Culture," Ponemon Institute, May 2016

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.**