THIRD ANNUAL 2016

Data Breach Industry Forecast

By Experian® Data Breach Resolution

EXECUTIVE SUMMARY

With the frequency and sophistication of security incidents continuing to advance at what seems like breakneck speed, it is essential that companies increase their data breach preparedness. Not only that, but the landscape has changed with hackers targeting organizations for different types of data that could be used for extortion or to simply cause harm. While traditional data breach threats remain, it is important that business leaders take note of emerging trends and update their data breach response plans accordingly.

In 2015, research from the Ponemon Institute revealed that while more companies now have a data breach response plan in place, many are still not confident in their ability to manage a significant incident.[1] Concerns regarding the effectiveness of response plans indicate a need for business leaders to reevaluate and audit their programs.

To help organizations prepare for what lies ahead and ensure incident response plans are ready for the evolving data breach environment, Experian Data Breach Resolution has outlined **five predictions** for what we can expect in 2016. Now in its third year, this Data Breach Industry Forecast report captures new trends and evaluates how previous Experian predictions panned out. The 2016 predictions are rooted in Experian's expertise in helping companies navigate more than 15,000 breaches over the last decade.

Based on our experience, we anticipate the top data breach issues and trends of 2016 to include the following:

- The EMV Chip and PIN liability shift will not stop payment breaches.
- Big healthcare hacks will make the headlines but small breaches will cause the most damage.
- Cyber conflicts between countries will leave consumers and businesses as collateral damage.
- 2016 U.S. presidential candidates and campaigns will be attractive hacking targets.
- Hacktivism will make a comeback.

1 The EMV chip and PIN liability shift will not stop payment breaches.

Although October 1, 2015, marked the official liability shift date for U.S. vendors to adopt EMV chip and PIN compatible payment terminals, it will not be a silver bullet against payment breaches. According to a study by Experian and the Ponemon Institute, just over half of executives in the payments sector believe chip and PIN will decrease the risk of a breach.[3]

According to research from the Ponemon Institute, 64 percent of executives believe it is more challenging to secure payment card information than other personal identifiable information.[3]

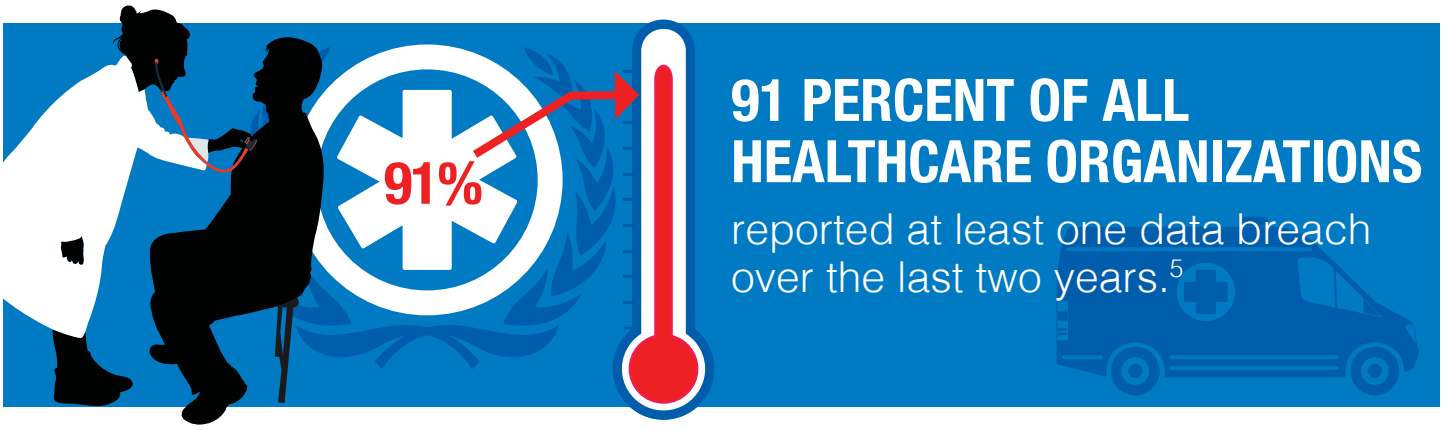
There are a number of reasons why these attacks may continue – one is that many retailers and other merchants have yet to fully adopt chip and PIN technology, which may still leave them vulnerable to the same malware attacks that continue to make headlines. A recent survey from the Hartford Financial Services Group found 86 percent of small businesses have not yet invested in equipment to accept chip and PIN cards, despite the liability shift deadline.[4] In addition to small businesses, distributed payment systems like gas stations and independent ATM networks are likely going to take significant time to adopt the system. In both cases, it's possible we could see the cost of breaches to these types of organizations increase in the coming year.

Another potential concern is imperfect implementation of EMV introducing previously unknown vulnerabilities that attackers could exploit. Anytime a major technology is adopted, it's possible that companies will make implementation errors that could leave them vulnerable to new types of attacks. Further, given the value of payments data, attackers may also look to other methods to steal this information that don't involve point of sale systems. Similar to what's happened in the European Union – where EMV has been adopted for some time – attacks may shift to focus on online transactions where cards don't need to be present.

The Takeaway:

Despite the EMV liability shift, payment-related breaches will still make headlines in 2016. Merchants may be vulnerable to attack during the transition from magstripe to EMV payment terminals, and newer technologies like mobile wallets will continue to be a target for hackers.

It is important for companies and consumers alike to realize new payment technologies are not a panacea for payment breaches and fraud. If anything, it's possible that e-commerce sites for retailers will bring the next wave of attacks. We've already started to see glimpses of this with the recent attacks on some retailers photo service websites.



2 Big healthcare hacks will make the headlines but small breaches will cause the most damage.

We predict that healthcare companies will remain one of the most targeted sectors by attackers, driven by the high value compromised data can command on the black market, along with the continued digitization and sharing of medical records. In 2016, sophisticated attackers will continue to focus on insurers and large hospital networks where they have the opportunity for the largest payoff. With the move to electronic health records (EHRs) continuing to gain momentum and becoming more widely accessible through mobile applications, the attack surface continues to grow.

Medical records are worth up to 10 times more than credit card numbers on the black market.[6]

There are also many more people in the system due to the Affordable Care Act, which leads to more available data to steal. However, behind the headlines lies a much more potentially concerning trend that we believe has been under-reported. While large breaches may be compromising millions of people's records in one fell swoop, smaller incidents caused by employee negligence will also continue to compromise millions of records each year. These incidents are often due to employees mishandling paper records or losing physical back-up of information.

The Takeaway:

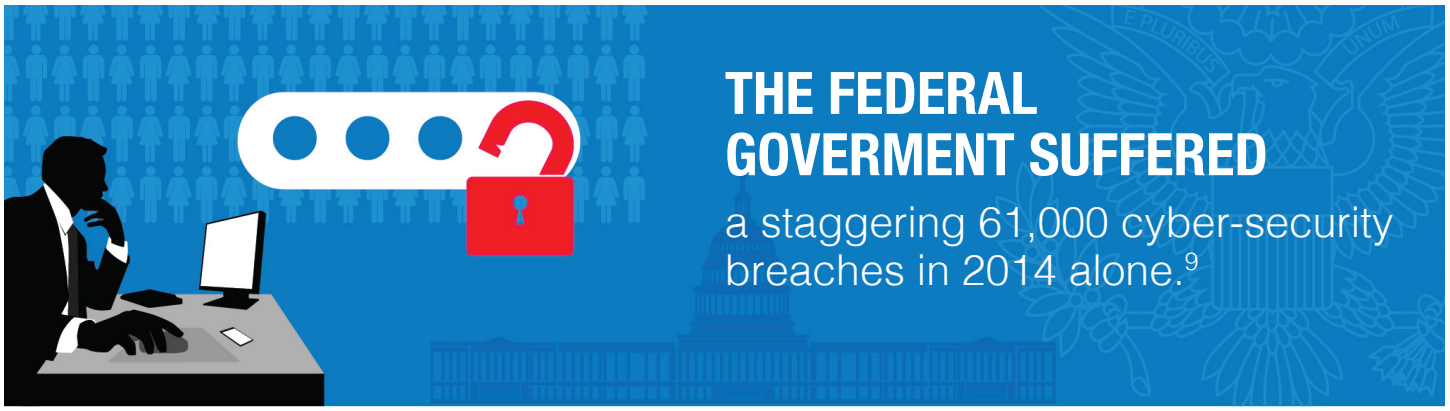
The healthcare sector will continue to be a focal point for attacks in the coming year because of the value of medical records on the black market. While credit card records continue to lose value on the dark web, medical records remain lucrative.

It's important that health organizations not only continue to invest in up-to-date security technologies, but also focus on training employees on proper data handling practices on a regular basis.

GROWTH IN CORPORATE EXTORTION

As the value of payment records decrease on the black market, more hackers will likely look to access data for extortion purposes or other scams in 2016. The large volume of data breaches over the past few years means the dark market is saturated with more personal records available than ever before. Credit card information can sell for a mere $12[7] and more consumers now have credit freezes on accounts, which makes it more difficult for criminals to access accounts for quick financial gain.

This may drive hackers to look for other means for financial gain. Corporate extortion is top of this list, with 38 percent of organizations reporting they've already been targeted by cyber-extortion.[8] Moving forward, it is anticipated that businesses will begin to account for the potential of extortion in their data breach preparedness planning, including having cyber insurance policies in place that incorporate protocols for how to negotiate with cybercriminals.



3 Cyber conflicts between countries will leave consumers and businesses as collateral damage.

Cybercrime is no longer the only concern when it comes to data breaches. As nation-states continue to move their conflicts and espionage efforts to the digital world, we are likely to see more incidents aimed at stealing corporate and government secrets or disrupting military operations. According to research from The Wall Street Journal, more than 60 countries have or are developing tools for computer espionage and attacks, and 29 countries now have formal military or intelligence units dedicated to cyber efforts.[10]

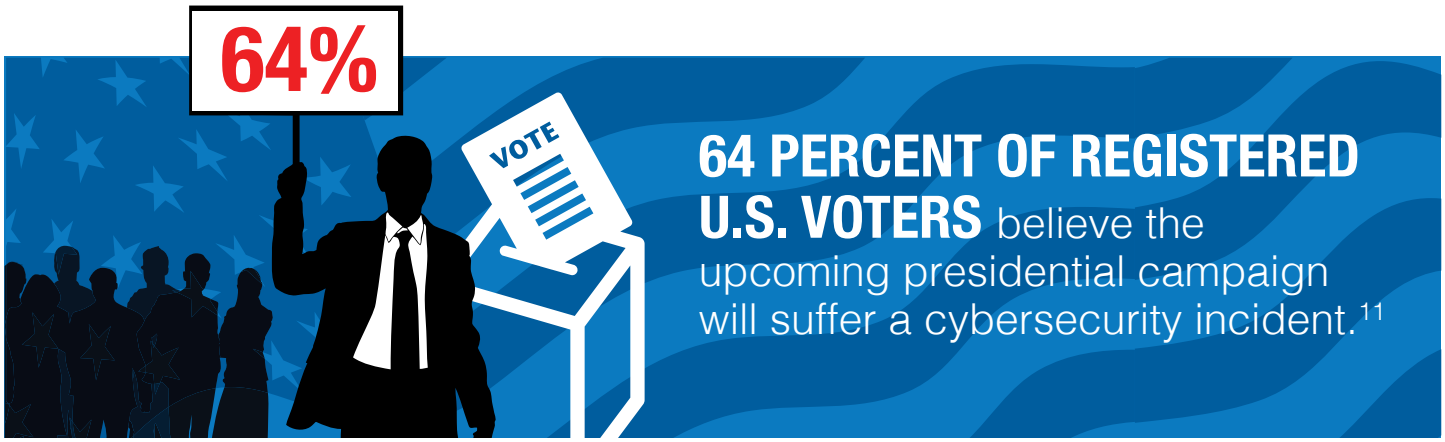
The U.S. Director of National Intelligence ranks cybercrime as the No. 1 national security threat, ahead of terrorism, espionage and weapons of mass destruction.[1]

However, just like in the physical world, these attacks are likely to cause collateral damage in the form of millions of innocent individuals having their information potentially exposed or businesses having their IP stolen. Looking ahead, we could see an increase in large public sector data breaches that will expose millions of personal records in the process, similar to what was seen with the 2015 Office of Personnel Management breach. While the OPM attackers were likely after specific information from only a subset of individuals affected by the incident, millions of people's personal information may have been exposed in the process.

These breaches are likely not going to be limited to the public sector. Many nation-state attacks may be targeting corporate entities as well, which could lead to lost employee or customer records in a similar manner.

The Takeaway:
There certainly needs to be continued discussion and consensus between countries on the proper rules of engagement in cyber-space. More importantly, companies involved in critical infrastructure or potentially sensitive political information should continue to invest in advanced threat protection.

Consumers who find themselves caught in the middle should take advantage of free identity theft protection services when offered to them after a known data breach and proactively monitor all accounts for suspicious activity.



4 2016 U.S. presidential candidates and campaigns will be attractive hacking targets.

We would be remiss if we didn't acknowledge this major event as an attractive target. With the looming 2016 U.S. presidential election dominating media coverage, it is likely that one of the presidential candidates, their campaigns and/or a major donor bases will be hacked. Because campaigns today are being won and lost online and are driven by big data analytics, the potential for a politically-motivated attacker to take aim is potentially significant. A hack of this kind could likely occur in the lead up to the election and could take many forms, from exposing secrets or embarrassing information about the candidates to outing the funding sources of super PACs.

There is already precedent for this type of attack. During the 2008 election cycle, Republican Vice Presidential Nominee Sarah Palin had her personal e-mail hacked with her private messages exposed.

The Takeaway:

Anytime there is a major activity or event, leaders involved should be prepared for a data breach. In this case, political organizations and campaigns should ensure that they are securing their systems and have incident response plans in place. If sensitive information about the campaign or donor information is exposed, it could cause a disruption or reputational damage.

MILLENNIAL WORKFORCE PRESENTS INFORMATION SECURITY THREAT

As more young adults enter the workforce, employers are faced with a challenge: balancing technology innovation and digital solutions with information security. Millennials are possibly best known for their frequent use of social-networking sites and mobile devices as a key part of their daily lives – including electronic sharing of information from the workplace. For example, the Wall Street Journal reports millennials often interact with colleagues through non-corporate channels and look for potentially more efficient external file-sharing solutions which may be less secure.

With unsanctioned technology solutions leveraged for a business environment, we may see employees continue to be a leading cause of data breaches in the coming years. Companies should take note of this and address it by ensuring employees receive regular security training and are familiar with what information should not be shared outside company walls. This is even more important when you consider that half of businesses surveyed report that data protection and/or privacy awareness programs are not provided as part of their new employee orientation process.[1]

THE WORD "HACKTIVISM" WAS FIRST COINED IN 1996 by "Omega", a member of the hacker collective Cult of the Dead Cow.[12]

5 Hacktivism will make a comeback.

In 2013, we saw a rise of hacktivism with groups like Anonymous and LulzSec targeting companies and organizations whose practices or policies they didn't agree with. However, over the past couple of years, these groups have tended to either scale back their efforts or saw their members arrested.

In the coming year, we are likely to see a resurgence in hacktivist activities, motivated by causing reputational damage to a company or cause. A couple of recent high-profile attacks provide an idea of what might come. For example, the individuals that claimed responsibility for the attack on Ashley Madison aimed to shut down the site's operations because they objected to the premise of the business and its poor security practices. Another example is the continued use of DDoS attacks by groups and lone wolves targeted at online gaming services to gain attention.

The Takeaway:

There are cyber criminals that are not motivated by financial gain. Any organization or group with a polarizing or controversial standing should be prepared for the possibility of an attack for the purpose of harm to the organization and/or its constituency. The impact of these types of incidents can often cause significantly more damage to individuals and are harder to resolve for the business. It is imperative that organizations and companies be prepared to respond to this type of security incident, and rethink their data breach response plans to prepare for all scenarios that can include extortion.

EXPECT MORE ENFORCEMENT ACTION FROM REGULATORS

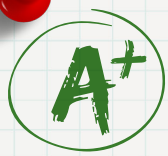
While the last several months saw increased scrutiny from regulators on what steps are being taken by companies to protect customer and employee data, this year companies can expect more direct enforcement actions from agencies.

The recent FTC v. Wyndham Worldwide case is a clear indication of movement in this area, as federal courts granted the FTC authority to require companies to securely store customer data and then punish them if they failed to do so.[13] After the FTC sued the hospitality company and three subsidiaries, alleging that data security failures led to three data breaches at Wyndham hotels in less than two years, a federal District Court denied Wyndham's motion to dismiss the action. In March 2015, the case was resolved after the U.S. Court of Appeals for the Third Circuit ruled in the Commission's favor.

As a best practice, companies should have an open line of communication with regulators to ensure they are doing their due diligence to protect customers and stay ahead of evolving security threats.

PREDICTIONS SCORECARD: HERE'S HOW WE DID ON 2015 PREDICTIONS

To hold ourselves accountable, last year we graded our 2014 predictions to determine which rang true at the end of the year. This year we did the same, with mixed results. Four out of six predictions from our 2015 Data Breach Industry Forecast made the cut this year with top marks:



PERSISTENT AND GROWING THREAT OF HEALTHCARE BREACHES

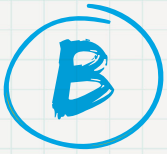
As predicted, healthcare data breaches continued to persist in 2015. Several media headlines as early as March reported 2015 as the year of healthcare breaches, citing attacks on Anthem, Premera BlueCross BlueShield and UCLA Health Systems. At the end of the day, healthcare data remains highly vulnerable given the value medical records have on the black market, which is why we believe healthcare attacks will continue in 2016.

MISSING THE MARK: EMPLOYEES WILL BE COMPANIES' BIGGEST THREAT

According to a February report from the Ponemon Institute, the number one leading cause of data security breaches resulted from non-malicious employee error.[14] Human error continues to be one of the leading causes of data breaches. We also saw that employee training programs continue to lag as a priority, indicating this will continue to be a source of breaches.

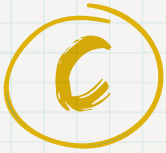
SHIFTING ACCOUNTABILITY: BUSINESS LEADERS UNDER INCREASED SCRUTINY

It is no secret that in 2015 there was an increase in scrutiny of corporate leadership's management of security after major incidents. A number of recent high-profile data breaches illustrate how large-scale attacks are often claiming the jobs of top staff, including CEO departures from Sony and Avid Life Media, the parent company of Ashley Madison.



FRESH BREACH SURFACE VIA THE INTERNET OF THINGS

While there haven't been many data breaches in this category, the Internet of Things (IoT) remains a top concern for cybersecurity executives. According to predictions from the International Data Corporation (IDC), within two years, 90 percent of all IT networks will face an IoT-based security breach.[15]



RISE-AND FALL-OF PAYMENT BREACHES

As the window closed for hackers to profit from attacks on brick-and mortar retailers looking to adopt chip and PIN technology, payment breaches continued throughout 2015. According to the 2015 annual Verizon Data Breach Report, point-of-sale intrusions ranked number one as the primary leading cause of a data breach.[16] Where we were misguided was in the timeline for the anticipated subsequent fall in payment breaches; criminals were not hyper targeting retailers leading up to the October chip and PIN deadline. We think that payment-related breaches may continue in the coming year but we still may see it dip as retailers transition and card-not-present fraud possibly increases.

SAFEGUARD YOUR PASSWORD: MORE HACKERS WILL TARGET CLOUD DATA

This prediction was challenging to grade ourselves on, as it largely depends on how the cloud is defined. For example, if a website represents the cloud, then the prediction definitely came to fruition as corporate websites were targeted on a regular basis. For the most part, however, cloud computing avoided the spotlight this year in terms of major security incidents.

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

Experian®

Footnotes:

1. "As Data Breach Occurrences Increase, How Ready Is Your Company? Third Annual Study on Data Breach Preparedness," Ponemon Institute, October 2015.
2. Data Security in the Evolving Payments Ecosystem, Ponemon Institute, 2015
3. "Data Security in the Evolving Payments Ecosystem," Ponemon Institute, April 2015.
4. "Fifth Annual Small Business Success Study," The Hartford, September 2015.
5. Identity Theft Resource Center
6. "Your medical record is worth more to hackers than your credit card," Reuters, September 2014.
7. "Underground Hacker Markets," Dell SecureWorks, 2014.
8. "Negotiating with Cybercriminals: 30% of Security Professionals Say They Would Pay for the Return of Their Data," ThreatTrack, March 2015.
9. These 5 Facts Explain the Threat of Cyber Warfare, TIME, June 2015
10. "Cataloging the World's Cyberforces," The Wall Street Journal, October 2015.
11. PKWARE poll, September 2015
12. Hacktivism 101: A Brief History and Timeline of Notable Incidents, Trend Micro Security News, August 2015
13. "Third Circuit rules in FTC v. Wyndham case," Federal Trade Commission, August 2015.
14. "Ponemon Institute's Survey on Data Security Breaches," Ponemon Institute, February 2015.
15. "IDC FutureScape: Worldwide Internet of Things 2015 Predictions," International Data Corporation, December 2014.
16. "2015 Data Breach Investigations Report," Verizon, April 2015.

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 protection products. In 2015, Experian Data Breach Resolution was named a market leader in the Forrester Research, Inc. report on data breach services. Experian Data Breach Resolution is active with the International Association of Privacy Professionals, the Health Care Compliance Association, the Ponemon Institute RIM Council, InfraGuard 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.