2015 Second Annual

Data Breach Industry Forecast

Experian®

Data Breach Resolution

EXECUTIVE SUMMARY

The growing prevalence of widely-publicized data breaches is sparking a change in the attitudes of business leaders and consumers when it comes to cybersecurity. Board members and the C-suite can no longer ignore the drastic impact a data breach has on company reputation. Meanwhile, consumers are demanding more communication and remedies from businesses after a data breach occurs. As a result, the topic is one of the highest priorities facing businesses and regulators in 2015.

For businesses, the risk of experiencing a data breach is higher than ever with almost half of organizations suffering at least one security incident in the last 12 months. To address this, 48 percent of organizations increased investments in security technologies in the same timeframe, and 73 percent acknowledged the likelihood of a breach by developing a data breach response plan.[1] Cyber insurance policies are also becoming more important to a company's preparedness plan, with the adoption rate more than doubling over the last year from 10 percent in 2013 to 26 percent in 2014.[2]

Where a year ago many organizations did not have a data breach response plan in place, it is encouraging that executives are better prioritizing this issue. However, much remains to be done as the data breach landscape and consumer sentiment continues to evolve. While several of the same issues are expected to persist in 2015, a few new trends are anticipated in the coming year. These changes will be driven by factors including implementation of new payment technology, continued rapid expansion of cloud and ecommerce, as well as the consistently high value of healthcare data on the black market.

The end of a year brings reflection as well as a chance to pause and look to the future. To help businesses understand implications of such changes and navigate the road ahead, Experian® Data Breach Resolution has developed six key predictions about how the data breach industry will evolve in 2015. These predictions are based on experience helping more than 3,000 companies manage breaches of all types in 2014 and conversations with leaders across the security landscape. With this mindset, we also looked back at how our 2014 predictions played out.

Based on our experience, the top data breach trends of 2015 include the following:

- **Rise-and Fall-of Payment Breaches**
  Adoption requirements for EMV "Chip and PIN" technology being implemented may drive an increase in the frequency of payment breaches as the window closes for hackers to profit from this type of attack on brick-and-mortar retailers. However, businesses should be wary of the potential for the new infrastructure creating a false sense of security for consumers.

- **Safeguard Your Password: More Hackers will Target Cloud Data**
  As more data is stored in the cloud, hackers are eager to capitalize on the value of consumer online credentials. There is an expected increase in cyber attacks to access consumer passwords and other data stored in the cloud.

The deadline for retailers to adopt EMV (Chip and PIN) credit card technology is October 2015 if they want to accept Visa or MasterCard payments.

- **Persistent and Growing Threat of Healthcare Breaches**
  The expanding number of access points to Protected Health Information (PHI) and other sensitive data via electronic medical records and the growing popularity of wearable technology makes the healthcare industry a vulnerable and attractive target for cybercriminals. Several factors suggest the healthcare industry will continue to be plagued with data breach headlines in 2015.

- **Shifting Accountability: Business Leaders Under Increased Scrutiny**
  Showcased by shifts in leadership at companies that suffered a public data breach in the last year, it is clear that security can no longer be viewed as just an IT issue. In 2015, scrutiny of corporate leadership's management of security may continue to increase in the form of legal and regulatory action after a major incident.

- **Missing the Mark: Employees Will Be Companies' Biggest Threat**
  Although businesses will increase focus on security protocols against external hackers this year, we predict that many will miss the mark on protecting against insider threat. Employees and negligence will continue to be the leading cause of security incidents in the next year.

- **Fresh Breach Surface via the Internet of Things**
  Like it or not, the Internet of Things (IoT) is spreading rapidly, offering a wide range of benefits for businesses looking to review data and optimize performance. More devices are being created with Wi-Fi capabilities and sensors that create the opportunity for everyday items — for example, car keys, alarm system or wearable devices — to relay information over the Internet and communicate with each other. As more companies adopt interconnected systems and products, cyber attacks will likely increase via data accessed from third-party vendors.

Confronting The Issue Of Data Breach Fatigue

The experience of being a victim to data breaches has created a substantial shift in consumer behaviors and attitudes over the last year, with increased expectations for swift notification and a decrease in the level of trust in the companies impacted. Consumers also send mixed signals to organizations — with many becoming more apathetic in a phenomenon coined as "data breach fatigue" and taking less action to personally protect themselves — whilst expressing heightened concern for identity theft.

In a 2014 study from the Ponemon Institute, more than one-third of consumers reported they ignored data breach notification letters, taking no action to protect themselves from fraud. However, most consumers continue to believe organizations should be obligated to provide identity theft protection (63 percent) and credit monitoring services (58 percent).[3]

To confront data breach fatigue, companies need to avoid treating the notification process as a compliance issue, and conduct sincere communication with customers. Notification letters should include an apology and a clear explanation of what happened, why it happened, and what consumers can do to protect themselves from fraud. This includes checking credit reports and monitoring financial or health records to identify any fraudulent activity.

TOP 6 DATA BREACH TRENDS FOR 2015

1. Rise-and Fall-of Payment Breaches

With the imminent adoption requirements for EMV "Chip and PIN" technology in the United States in October 2015, the window may be closing for hackers to easily profit from point-of-sale attacks on brick-and-mortar retailers. Today, U.S.-based retailers face a perfect storm of having information that is an attractive target to attackers and the availability of malware capable of compromising payment systems being sold on the black market. We expect a continued influx of payment breaches in the near-term before the new system is implemented late next year.

In the interim, larger retailers will continue to take steps to harden their systems to be less vulnerable to attacks. However, despite increased security efforts, attackers may look for new ways to compromise these companies given how profitable the payoff can be. Because the October 2015 deadline to adopt the new technology has been publicly announced, cyberthieves have likely already identified vulnerabilities they can target in the new infrastructure. As this technology is viewed by many as the panacea for retail breaches, consumers could easily get a false sense of security.

We also expect to see attacks on smaller regional chains that could be more vulnerable but still provide a significant amount of payment cards. Even after the October deadline for merchants to implement new, more secure payment infrastructure or face being responsible for fraudulent charges, smaller vendors may be slow to adopt the new system. This means payment breaches will likely persist, but the likelihood of another mega credit card breach due to POS malware will be significantly reduced.

The Takeaway: The window is closing for traditional retail payment breaches, meaning there may be a rise in criminal activity in the coming months before more secure payment technologies are implemented. However, once Chip and PIN technology is adopted, it won't be long before cyber thieves identify new vulnerabilities to target. Either way, retailers need to prepare for the likelihood of a breach by hardening the security of their infrastructure and ensuring there is a proper incident response plan in place. The risk of credit card companies and banks filing lawsuits against breached retailers will also be motivation for companies to invest in security sooner rather than later.

2. Safeguard Your Password: More Hackers will Target Cloud Data

In 2015, we expect an increase in breaches involving the loss of usernames, passwords and other information stored in the cloud. Cloud services have been beneficial to both consumers and business productivity. However, as more information gets stored in the cloud and consumers rely on online services for everything from mobile payments and banking to photo editing and commerce, they become a more attractive target for attackers.

In fact, a recent study found a Twitter account is worth more on the black market than a credit card number[4] and stolen identities including online credentials are worth upwards of $25 per record on the black market.[5]

We expect this increase in hackers targeting online credentials such as consumer passwords and usernames to gain keys to the castle — with the likelihood that compromising one record can often give access to all sorts of other information stored online.

Beyond online credentials, loss of other personal information remains concerning if still underreported. Breached emails often lead to spear phishing attacks or SPAM and the loss of personal information like name, address, date of birth and Social Security numbers can be used as part of synthetic identity theft.

The Takeaway: There may be an increase in cyber attacks this year to access consumer passwords and other data stored in the cloud. To combat this, incident response plans should include considerations of how to reset user

passwords on a massive scale and send email promptly to all potentially affected. The need to maintain trust necessitates being transparent with customers.

3. Persistent and Growing Threat of Healthcare Breaches

We expect healthcare breaches will increase — both due to potential economic gain and digitization of records. Increased movement to electronic medical records (EMRs), and the introduction of wearable technologies introduced millions of individuals into the healthcare system, and, in return increased, the potential for data breaches.

Healthcare organizations face the challenge of securing a significant amount of sensitive information stored on their network, which combined with the value of a medical identity string makes them an attractive target for cybercriminals.

The problem is further exasperated by the fact that many doctors' offices, clinics and hospitals may not have enough resources to safeguard their patients' PHI. In fact, an individual's Medicare card — often carried in wallets for doctors' visits — contains valuable information like a person's Social Security number (SSN) that can be used for fraud if in the wrong hands. Currently, we are not aware of any federal or law enforcement agency which tracks data on SSN theft from Medicare cards, but the

Boom In State-Level Regulatory Action

In the absence of federal regulatory action for standardized data breach notification requirements, states may experiment with data breach laws in the coming year, from adjusting timing and content of notification, to defining personal data, and requirements to alert media and regulators. Unfortunately, for companies with customers in multiple states there is no one-size-fits-all approach to notification that meets each standard. Currently, U.S. businesses face a patchwork of data breach laws across 47 states, along with the District of Columbia and Puerto Rico. Three states remain without data breach notification laws (Alabama, New Mexico and South Dakota).

This year, in light of recent breaches several states are likely to adopt new standards that expand the definition of personal data to include email and password information and non-HIPAA related health data, such as health insurance policy numbers and subscriber identification numbers. Under these proposals, the expanded definition of personal data could trigger breach notices in more frequent circumstances. It is important to maintain a comprehensive and regularly updated data breach response plan to ensure companies are prepared to meet these new requirements and various standards.

Policymakers at the state and federal level agree — companies need to be prepared to respond to a breach. In fact, after reporting that more than 500 million financial records had been stolen by hackers in the past 12 months, Joseph Demarest, assistant director in the FBI's Cyber Division issued a warning saying, "You're going to be hacked. Have a plan." State attorneys general in California, New York and Illinois have each called on companies to have a breach response plan in place that includes the offering of identity theft protection services to affected customers.

problem is widely acknowledged.

The potential cost of breaches for the healthcare industry could be as much as $5.6 billion annually.[6]

This year, Reuters reported that the FBI released a private notice to the healthcare industry warning providers that their cyber security systems are lax compared to other sectors. A memo reportedly stated, "the healthcare industry is not as resilient to cyber intrusions compared to financial and retail sectors, therefore the possibilities of increased cyber intrusions is likely." According to the Ponemon Institute, 72 percent of healthcare organizations say they are only somewhat confident (32 percent) or not confident (40 percent) in the security and privacy of patient data shared on HIEs.[7]

The Takeaway: Healthcare organizations will need to step up their security posture and data breach preparedness or face the potential for scrutiny from federal regulators. Reported incidents may continue to rise as electronic medical records and consumer-generated data adds vulnerability and complexity to security considerations for the industry.

4. Shifting Accountability: Business Leaders Under Increased Scrutiny

Where previously IT departments were responsible for explaining security incidents, cyber attacks have expanded from a tech problem to a corporate-wide issue. With this shift, business leaders are being held directly accountable for data breaches. Executives at the highest levels are under scrutiny about security posture and their response to a breach from stakeholders, regulators and consumers. Recent mega breaches have showcased the significant pressure for management teams to brush up on their knowledge on data breach preparedness or face the threat of being ousted from the company.

In 2015, scrutiny of corporate leadership's management of security may continue to increase in the form of critical media coverage and legal and regulatory scrutiny in the wake of a major incident. We also expect to see more definitive action taken by boards to hold company leadership accountable.

Looking ahead, senior executives will be expected to have a better understanding of the data breach response plan, comprehension of new technologies and security protocols in the workplace and have a clearly-defined chain of response should a breach occur. This often doesn't exist today. According to a recent survey by the Ponemon Institute, 17 percent of senior executives are currently not aware of whether or not their organization had suffered a data breach in the last year.[8]

The Takeaway: Data breaches need to be managed as a corporate-wide risk in 2015. Decision-makers at the C-suite level should have an active role in preparing for a data breach and how to respond. They also should increase allocated resources to data security, or else face the consequences of appearing irresponsible to constituents and stakeholders.

5. Missing the Mark: Employees Mistakes Will Be Companies' Biggest Threat

Although there is heightened sensitivity for cyber attacks amongst business leaders, a majority of companies will miss the mark on the largest threat: employees. Between human error and malicious insiders, time has shown us the majority of data breaches originate inside company walls. Employees and negligence are the leading cause of security incidents but remain the least reported issue. According to industry research, this represented 59 percent of security incidents in the last year.[9]

Expect a rise in legal and regulatory scrutiny in 2015.

In 2015, people-based breaches will continue to be the leading cause of compromises but will receive the least attention. Investments will favor new technologies capable of helping better prevent intrusions and the exfiltration of data from attackers. Currently only 54 percent of organizations report they conduct security awareness training for

employees and other stakeholders who have access to sensitive or confidential personal information.[10] Making a significant dent in the number of breaches in 2015 will require companies to pay more attention to raising the security intelligence of employees.

U.S. companies reported $40 billion in losses from unauthorized use of computers by employees last year.[11]

The Takeaway: Despite all signs pointing to employees as the largest threat to a company's security, business leaders will continue to neglect the issue in favor of more appealing security technologies in 2015. As a result, many companies will miss the mark on fighting the root cause of the majority of breaches. Organizations that implement regular security training with employees and a culture of security committed to safeguarding data will be better positioned for success.

6. Rise in Third-Party Breaches via the Internet of Things

The next leak from the office water cooler won't be caused by employee gossip. Technology advancements means the Internet of Things (IoT) is changing how people interact with everyday items. Growing in popularity as a way for businesses to measure data in new ways, the IoT allows us to gather and process valuable information from machines and other physical objects.

According to Gartner, the IoT will grow to 26 billion units installed in 2020 representing an almost 30-fold increase from 0.9 billion in 2009.[12] With more companies looking to leverage the IoT by gathering, storing and processing data from billions of objects and devices, there are more points of vulnerability for this information to be targeted by hackers. As a result, we expect an increase in cyber attack campaigns initiated by IoT-compromised devices and interconnected systems adopted by organizations, including everything from sensor networks and work meters to consumer devices such as routers and NAS storage.

The Takeaway: As companies adopt more interconnected products and systems, the Internet of Things could usher in the next wave of large third-party breaches. Businesses looking to take advantage of data available from the IoT need to emphasize risk management and security with third-party vendors that provide or have access to the same information.

Medical Identity Theft A Growing Concern

Cybercriminals looking to capitalize on a bigger payout may continue to target the healthcare industry for access to patients' Protected Health Information (PHI). Industry reports reveal medical identity theft has now claimed more than 1.8 million U.S. victims, granting hackers the ability to gain medical services, procure drugs, and defraud private insurers and government benefit programs.[13]

Experian® Data Breach Resolution is currently working with organizations like the Medical Identity Fraud Alliance (MIFA) to take the lead on tackling this issue. MIFA is the first public/private sector-coordinated effort with a focused agenda that unites all the stakeholders to jointly develop solutions and best practices for fighting medical identity fraud.

"Medical identity theft is a serious threat that needs to be prioritized by healthcare organizations, regulatory groups and consumers," said Ann Patterson, senior vice president of the Medical Identity Fraud Alliance. "There is no single solution for fraud prevention, meaning we must take a collaborative approach to solving the issue. Industry and government must work together to develop holistic strategies pertinent to the fight against fraud, and consumers should take an active role in advocating for system-wide reform."

A LOOK AT 2014 PREDICTIONS — HERE'S HOW WE DID

We started out last year with some bold predictions for 2014 in our 2014 Data Breach Industry Forecast white paper. Here is a look at how we did:

☒ **Data Breach Cost Down — But Still Impactful**

With the average data breach costing organizations $3.5 million, the financial impact of data breaches actually increased this year. According to annual research from the Ponemon Institute, the average cost paid for each lost or stolen record containing sensitive and confidential information globally increased more than 9 percent from $136 in 2013 to $145 in 2014. The cost per record increased to $195 for companies in the U.S.[14]

☑ **Will the Cloud and Big Data = Big International Breaches?**

This year was fraught with mega breaches dominating the media headlines. Widely publicized data breaches suffered by e-commerce and cloud technology companies underscore the need for web-based and cloud companies to secure data.

☑ **Healthcare Breaches: Opening the Floodgates**

The sheer size of the healthcare industry led to an increase in widely publicized breaches this year. Early in 2014, attempted attacks sparked concern early about the overall vulnerability of healthcare organizations, and a recent breach exposed medical records for 4.5 million patients from 206 hospitals across 23 states. Even more impressive, the healthcare industry accounted for 42 percent of major data breaches reported in 2014 according to the Identity Theft Resource Center.

☑ **A Surge in Adoption of Cyber Insurance**

To increase their security posture, more and more companies have been adopting cyber insurance as part of their preparedness plan. According to the Ponemon Institute, the adoption rate for cyber insurance more than doubled from 10 percent to 26 percent over the past year.[15]

☑ **Breach Fatigue: Rise in Consumer Fraud?**

Data breach fatigue was a widely-discussed topic in 2014, with reporters from nationally-ranked media outlets like NPR, Bloomberg and the Wall Street Journal buzzing about the issue. And after 62 percent of consumers reported they had received at least two data breach notifications involving separate incidents in the past two years, perhaps surprisingly the most frequent response was inaction. According to the Ponemon Institute, 32 percent of consumers do nothing after they are notified of a data breach.[16]

☑ **Beyond the Regulatory Checkbox**

As predicted, state regulators stepped up efforts to engage companies on data breach response in 2014. But a national breach law still did not pass. Though this is still being discussed.

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

Footnotes:

[1] "Is Your Company Ready for a Big Data Breach?" Ponemon Institute, September 2014.

[2] "Is Your Company Ready for a Big Data Breach?" Ponemon Institute, September 2014.

[3] "Aftermath of a Mega Data Breach: Consumer Sentiment," Ponemon Institute, May 2014.

[4] "Markets for Cybercrime Tools and Stolen Data," Juniper Networks and the RAND Corporation, March 2014.

[5] "Hackers Sell Health Insurance Credentials, Bank Accounts, SSNs and Counterfeit Documents, for over $1,000 Per Dossier," Dell SecureWorks, July 2013.

[6] "Fourth Annual Benchmark Study on Patient Privacy & Data Security," Ponemon Institute, March 2014.

[7] "Fourth Annual Benchmark Study on Patient Privacy & Data Security," Ponemon Institute, March 2014.

[8] "Is Your Company Ready for a Big Data Breach?" Ponemon Institute, September 2014.

[9] "2013 Cost of Data Breach Study: Global Analysis," Ponemon Institute, May 2013.

[10] "Is Your Company Ready for a Big Data Breach?" Ponemon Institute, September 2014.

[11] "2014 Insider Threat Survey," SpectorSoft, August 2014.

[12] "Forecast: The Internet of Things, Worldwide," Gartner, Inc., December 2013.

[13] "2013 Survey on Medical Identity Theft," Ponemon Institute, September 2013.

[14] "2014 Cost of Data Breach Study: Global Analysis," Ponemon Institute, May 2014.

[15] "Is Your Company Ready for a Big Data Breach?" Ponemon Institute, September 2014.

[16] "Aftermath of a Mega Data Breach: Consumer Sentiment," Ponemon Institute, May 2014.

About Experian Data Breach Resolution

Experian Data Breach Resolution, powered by the nation's largest credit reporting agency, is a leader in helping businesses plan for and mitigate consumer risk following data breach incidents. With more than a decade of experience, Experian Data Breach Resolution has successfully serviced some of the largest and highest-profile breaches in history. The group offers swift and effective incident management, notification, call center support and reporting services while serving millions of affected consumers with proven credit and identity protection products. In 2013, Experian Data Breach Resolution received the Customer Service Team of the Year award from the American Business Awards. Experian Data Breach Resolution is active with the International Association of Privacy Professionals, the Health Care Compliance Association, the American Health Lawyers Association, the Ponemon Institute RIM Council and InfraGuard and is a founding member of the Medical Identity Fraud Alliance. For more information, visit www.experian.com/databreach.