Experian®

DATA BREACH RESOLUTION

2014 Data Breach Industry Forecast

EXECUTIVE SUMMARY

The number of data breaches both experienced and reported is expected to continue to rise, with new security threats and regulations pushing for more transparency on the horizon. All signs are pointing to 2014 being a critical year for companies to better prepare to respond to security incidents and data breaches.

Over the past decade, we have seen an explosion of security incidents impacting millions of consumers worldwide. Throughout 2013, there were many significant data breaches and this shows no sign of slowing in the upcoming year with healthcare, energy, financial services, retail and telecom industries continuing to be top targets. In fact, this past year marked the single, largest breach to date.

While more than half of organizations are armed with data breach preparedness plans, not everyone is prepared.[1] This is unfortunate because the assumption should be that a data breach is likely to happen.

To better understand what may lie ahead, Experian® Data Breach Resolution has developed six key predictions for how concerns about data breaches will evolve over the course of 2014. It is imperative that companies and organizations understand the evolving data breach environment and ensure their response plans are continuously enhanced to address emerging issues.

The top data breach trends of 2014 are anticipated to include the following:

- **Data Breach Cost Down - But Still Impactful**
  The cost per record of a data breach is likely to continue to decline, largely due to increased awareness among organizations of how to prepare for and mitigate the damage caused by any single incident. However, security incidents and other breaches can still cause significant business disruption if not properly managed and the number of reported breaches still may rise.

- **Will the Cloud and Big Data = Big International Breaches?**
  International data breach response plans will be essential in 2014 as European Union regulations continue to take shape and will be enforced based on where the customer lives rather than where the data is located. With the rise of the cloud, data is now moving seamlessly across borders making the potential for complex, international breaches more possible. In response, organizations will begin looking for internationally savvy privacy attorneys to help guide them through the new regulations and foreign jurisdictions.

- **Healthcare Breaches: Opening the Floodgates**
  With the addition of the Healthcare Insurance Exchanges, millions of individuals will be introduced into the healthcare system and in return increase the vulnerability of the already susceptible healthcare industry. When combined with new HIPAA data breach compliance rules taking shape, the healthcare industry is likely to make the most breach headlines in 2014.

- **A Surge in Adoption of Cyber Insurance**
  Currently, one-third of companies have purchased cyber insurance, according to a recent Ponemon study, and the study indicates there will be a 50 percent growth in policies purchased in the next year.[2]

- **Breach Fatigue: Rise in Consumer Fraud?**
  As breach notifications become more frequent, consumers may begin to suffer from "data breach fatigue." This may drive them to be less likely to take steps to protect themselves and lead to increasing levels of fraud and identity theft.

- **Beyond the Regulatory Checkbox**
  Even though a federal data breach law isn't slated for this upcoming year, state regulators are likely to ramp up efforts to engage companies on data breach responses. Along with the potential for increased fines, this engagement could provide an opportunity for more open communication and partnerships, which will help protect customers from harm.

TOP 6 DATA BREACH TRENDS FOR 2014

1) Data Breach Cost Down - But Still Impactful

As more and more organizations learn how to identify and respond to security incidents and data breaches, the cost per record of a data breach will probably continue to trend downward. Last year, according to the Ponemon Institute, the cost per record dropped from $194 to $188.[3] The key factors for the reduction include organizations having a strong security posture with incident response plans in place.

Presumably, better prepared companies are more effective at managing consumer concerns after an incident and in return can reduce the costs due to customer churn. Strong preparations also allow companies to be much more cost efficient in engaging outside consultants in managing a breach. Furthermore, many companies will offset the cost of incident response through cyber insurance policies.

The Takeaway:

A data breach still affects the bottom line so organizations cannot let their guard down. For small businesses, this can shut the doors. The better prepared a business is, the more likely that financial losses can be contained.

2) Will the Cloud and Big Data = Big International Breaches?

The data breaches of tomorrow are likely to be global in nature, adding significant complexity to the data breach response process. With the rise of cloud computing, significant quantities of sensitive data now travel across national borders in the blink of an eye. Large data centers host data from citizens all over the world. Yet, while these data flows are global, the data breach laws and cultural norms for responding to an incident are local. This makes responding properly to a large breach a significant compliance challenge.

Notifying individuals and providing some sort of fraud or identity protection in multiple countries will be increasingly important but complicated. With the European Union likely to pass more stringent regulations, the frequency of reported international data breaches is likely to explode. Most U.S. based organizations are not ready for this aspect of a data breach nor are the wide variety of consultants and providers that help them resolve a breach. The door is open to a burgeoning opportunity for industry players to fill a strong need.

The Takeaway:

The biggest challenge for companies will be awareness of each country's regulations and complying with all of them. Privacy attorneys who work in foreign jurisdictions are best suited to help companies understand the global notification responsibilities after a breach.

Stay tuned for more widespread European Union notification laws.

---

3) Healthcare Breaches: Opening the Floodgates

The healthcare industry, by far, will be the most susceptible to publicly disclosed and widely scrutinized data breaches in 2014. The sheer size of the industry makes it vulnerable when you consider that as Americans, we will spend more than $9,210 per capita on healthcare in 2013.[4] Add to that the Healthcare Insurance Exchanges (HIEs), which are slated to add seven million people into the healthcare system, and it becomes clear that the industry, from local physicians to large hospital networks, provide an expanded attack surface for breaches.

Further, the healthcare industry must also comply with new data breach and privacy requirements in the HIPAA Omnibus Rule, which is likely to increase fines and headlines about incidents. As organizations have learned with the new rule, they have to determine the probability of the Protected Health Information (PHI) being compromised, regardless of

ENCRYPTION IS NOT OPTIONAL

You've probably heard it a billion times: encrypt, encrypt, encrypt. But what does that really mean? Does it mean encrypt laptops and desktops and that's all? It may have meant that in the past but some companies are now encrypting data that travels between servers, computers and internal data.

Encrypting internal and traveling data may be expensive and time-consuming. But in light of all the breaches and federal government monitoring, it may be worthwhile. Laptops and desktops, however, aren't optional. They should be encrypted. Organizations should also keep up with IT security and install the latest software to protect their systems.

But technology alone isn't the answer. Numerous breaches are caused by insiders. In these cases, an employee purposely steals sensitive consumer data or carelessly opens a link and infects his or her company's systems. As a result, it's a good practice to establish procedures for safeguarding consumer data and limiting access to that data to staff members who truly need it to perform their job.

whether or not it would cause harm to the affected individuals.

Medical identity theft claimed more than 1.8 million U.S. victims before the end of 2013.[5]

The problem is further exasperated by the fact that many doctors' offices, clinics and hospitals are not in the data management business and therefore do not have enough resources to safeguard their patients' PHI. When combined with the soaring cost of medical identity theft caused by data lost in a breach, the healthcare industry is facing a perfect storm that could cause significant business disruption.

The Takeaway:
Healthcare organizations are entering a new frontier. Reported incidents will rise and regulations will force teams to re-evaluate data management procedures or face heady fines. Preparation is not just nice to have, it is a must.

4) A Surge in Adoption of Cyber Insurance
Many companies will look beyond just investing in technology to protect against attacks and towards the insurance market to manage financial ramifications of breaches. According to a recent Ponemon study, one-third of companies already have cyber insurance and the study estimates there will be a 50 percent growth in policies purchased in the next year.[6] When combined with the expected $1.3 billion in annual premiums in 2013,[7] the cyber insurance industry is likely to experience boom times.

While this trend should not be interpreted as companies waving the white flag at protecting against security threats, it does demonstrate the need to think beyond the traditional technology-centric "castle and moat" strategy. Cyber insurance not only provides a financial remedy, the process of evaluating coverage helps many companies improve their security posture and preparedness.

Furthermore, companies are likely to see a growing variety of coverage options as more corporate insurance providers enter the market. This will likely include policies geared at different market segments. In particular, the small- and medium-size business (SMB) segment is likely to see new specific policies and outpace the adoption when compared to other sectors. In part, this adoption will be driven from the need for SMBs to manage breaches while not having the in-house expertise or resources to manage the aftermath. Most policies provide access to the external legal, notification and technical expertise needed to manage these incidents.

The Takeaway:
Cyber insurance will start to become a must-have for companies. With the insurance industry evolving at breakneck speed, businesses that already have coverage should examine current policies and ensure they meet their evolving needs or shop around as more choices become available.

Small businesses experienced a 300% increase in cyberespionage attacks from 2011 to 2012.[8]

5) Breach Fatigue: Rise in Consumer Fraud?
Each day there are security incidents that go unreported, but as laws are changing and awareness is growing, more and more breaches are expected to be made public. As the number of reported breaches in the media increases and the frequency of notifications that consumers receive grow, they may become apathetic towards the subject. Consumers will surely give little attention to the severity of being affected by a breach and the importance of following the directions in notification letters.

With an estimated one out of four Americans receiving a breach notice,[9] it is possible consumers will get tired of hearing about breaches, leading to "data breach fatigue." This fatigue could lead to significantly more harm by causing fewer consumers to take action to protect themselves after an incident, which could result in higher levels of fraud. This includes failure to reset passwords or accounts that may have been compromised, not being extra vigilant watching for targeted phishing attacks or not taking advantage of credit monitoring or other fraud prevention tools provided by the affected company.

The Takeaway:
Notification is more than a courtesy. Letters need to be clear and digestible for consumers to encourage action. The customer mindset today may also warrant additional outreach approaches in addition to a letter to achieve action. In the end, it is in the company's best interest to do its utmost to help their customers protect themselves.

6) Beyond the Regulatory Checkbox: Partnering with Officials
Watch for state regulators and law enforcement to turn a new leaf this year. In the absence of significant action on the federal level, many state Attorneys General are devoting significant attention to helping organizations better manage breaches. This includes expanded enforcement action, but also opportunities to share best practices in helping prevent incidents and protect consumers.

California Attorney General Kamala Harris recently issued a report on medical identity theft urging the healthcare industry to use the federal Affordable Care Act as a window of opportunity to

DON'T FORGET THE LITTLE GUY

Breached organizations don't always fall into a neat little category. A breach can occur at any company, government agency, healthcare provider or insurer. As a result, organizations that experience a breach have customers or patients from every walk of life. They may be young, old, educated, wealthy, below poverty-level and from any ethnicity.

Therefore, companies that offer identity protection solutions should be able to cover every demographic. But that's not always the case. Many identity theft or credit monitoring products can only monitor adults with a credit history. Yet more often than not, breached companies have customers with small children or young adults with no credit history. Children, in fact, have a 51 percent higher chance of becoming a victim of identity theft than adults.[10]

Organizations need to be selective about who they choose to provide identity protection. There are breach resolution providers that have identity protection solutions for children, families and adults with no credit history whatsoever. But they must be sought out. That's why selecting a breach provider before you suffer a breach is a smart move.

become more proactive in preventing medical identity theft.[11]

Don't expect a national breach law to pass in 2014, although one may be coming by the end of the decade.

In Vermont, the Attorney General's office assists small businesses that want to improve the safekeeping of their customers' data. Don't be surprised if other Attorneys General announce similar programs. Likewise, local municipalities may also jump on the bandwagon.

An exception, however, is healthcare organizations and their business associates. They have to follow the new federal HIPAA Omnibus Rule and if found in violation of the rule, will experience strict penalties.

The Takeaway:
For companies and organizations that suffer an incident, communicating early and often with the appropriate regulatory offices can be beneficial in the long term and potentially reduce the possibility of regulatory action. Not only will officials likely be open to the call, they may be waiting.

SURGE IN CLASS-ACTION LAWSUITS?

There's a sea of change going on in U.S. courtrooms today and it doesn't look good for companies and non-profit organizations. More and more judges are reacting favorably to class-action lawsuits brought on by data breach victims. In the past, the burden of proving actual damages had been difficult for plaintiffs. But, the tipping point for demonstrating actual or potential harm may be changing due to recent rulings that have provided payments to the full breach population rather than just to the victims of fraud or identity theft.

The likelihood of a data breach is no longer a question; it is almost a certainty. But the recent settlements have significantly impacted the magnitude of future data breach rulings. Next year may be the year of the plaintiff and we could see a surge in class-action lawsuits.

"As more and more data breaches are reported, companies face an increased risk of enforcement by the government or private class actions, and regardless of the outcome of these cases, the costs can be staggering, as can the harm to reputation. There are steps companies can take to help optimize their risk levels, including benchmarking their security practices, policies and procedures, as well as conducting mock data breaches, including table top exercises," according to Andrew B. Serwin, Partner, Global Privacy and Data Security Practice Group at Morrison & Foerster LLP.

Footnotes:

1 Is Your Company Ready for a Big Data Breach, Ponemon Institute, April 2013

2 Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age, Ponemon Institute, August 2013

3 2013 Cost of Data Breach Study: Global Analysis, Ponemon Institute, May 2013

4 National Health Expenditure Projections, 2011-2012, Centers for Medicare and Medicaid Services

5 2013 Survey on Medical Identity Theft, Ponemon Institute, September 2013

6 Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age, Ponemon Institute, August 2013

7 The Betterley Report Cyber/Privacy Insurance Market Survey, 2013

8 Symantec Internet Security Threat Report, April 2013

9 McAfee and the National Cyber Security Alliance, September 2012

10 Child Identity Theft, Carnegie Mellon CyLab, 2013

11 Medical Identity Theft: Recommendations for the Age of Electronic Medical Records, Kamala D. Harris, Attorney General, California Department of Justice, October 2013