BREACH BAROMETER REPORT: YEAR IN REVIEW

2016 Averaged at Least One Health Data Breach Per Day, Affecting More Than 27M Patient Records

Protenus, Inc. in Collaboration with DataBreaches.net

Introduction

The healthcare industry has been plagued by breaches involving patient or health data throughout 2016, with hacking and ransomware incidents reminding us how vulnerable protected health information (PHI) remains. We'd love to tell you that by the end of the year things were starting to improve, but unfortunately that wasn't the case. Patient data can still be easily obtained and used maliciously, by insiders and external actors alike. Even as healthcare leaders became increasingly aware of the importance of health data protection, the number of breach incidents remained relatively steady each month of the year, highlighting the continued threat to patient data.

If 2016 trends continue, 2017 can expect to see a continued average of at least one health data breach disclosed per day. This retrospective aims to examine 2016 with an eye towards lessons learned and a way forward for protecting patient privacy.

Overview of 2016 Findings

Our analysis is based on 450 incidents either reported to HHS or disclosed in media or other sources during 2016. With more than one health data breach per day for the entire year, these breaches resulted in 27,314,647 affected patient records. Information was available for 380 of these incidents.

The largest health data breach reported in 2016 was the Banner Health[1] hacking incident with 3.62 million affected patient records. As Figures 1 and 2 show, there was no linear trend in either the number of breach incidents or patient records breached per month. June and August were the worst months in terms of total number of breached patient records, while November was the worst month in terms of number of breaches disclosed.

[1] Excludes an incident involving 10.3 million records hacked from a health plan insurer's vendor because no one ever accepted responsibility for ownership of the records. Those records re included, however, in our other analyses for the year.

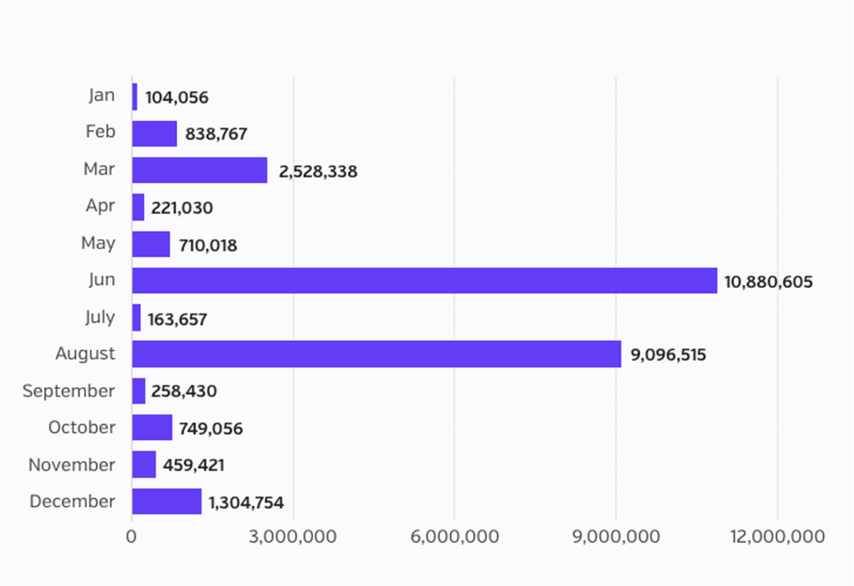

Figure 1. Number of Records Breached Per Month in 2016

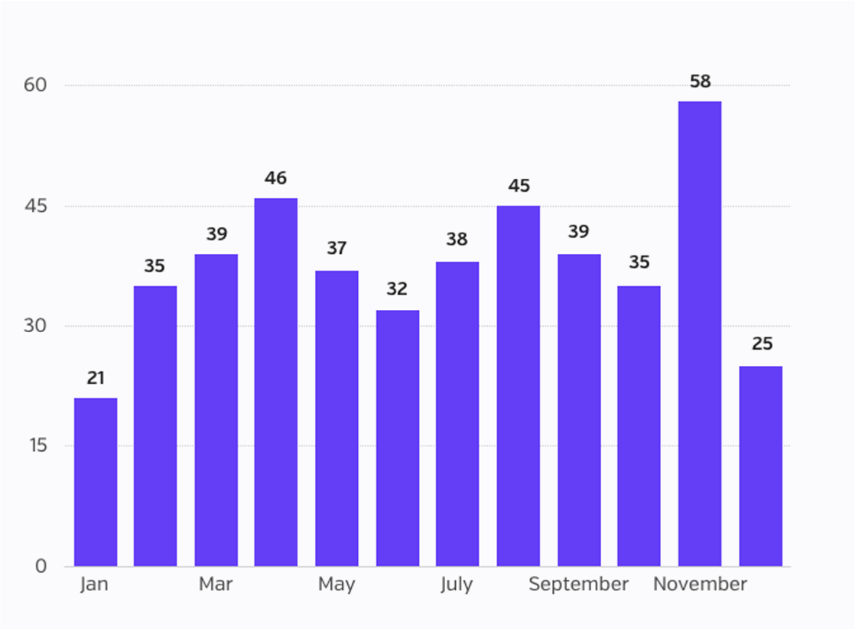

Figure 2. Number of Breaches Involving Health Data Disclosed Per Month in 2016[2]

[2] Graph represents partial data for the month of December. There are likely some breaches that may have been reported but have not yet appeared on HHS's breach tool or in the media by our December 31 cutoff date.

Insiders Responsible for 192 Health Data Breach Incidents

43% of the 2016 health data breaches (192 incidents) were a result of insiders. For the 162 incidents for which we have more detailed numbers, 2,000,262 patient records were affected. For the purpose of our analyses, we characterized insider incidents as either insider-error or insider-wrongdoing. The former included accidents and anything without malicious intent that could be categorized as "human error." Insider-wrongdoing included employee theft of information, snooping in patient files, and other cases where employees appeared to have knowingly violated the law.

99 of these incidents were a result of an insider-error or accident, while 91 incidents were a result of wrongdoing. In two cases, there was insufficient information to determine whether the incidents should be coded as error or wrongdoing.

As Figure 3a depicts, the average number of breached patient records due to insider-error were more than three times the number attributed to insiders with malicious intent. However, this figure is distorted by two large insider-error incidents in August and December, which, when removed, shows the two categories to have roughly similar averages (see Figure 3b). While it is reassuring that not all insider breaches are with ill-intent, healthcare organizations need to make employee training, frequent reminders, and re-training a priority.

In one incident, hospital employees were potentially inappropriately accessing patients' medical information for years without being detected, because the hospital didn't have technology in place to monitor or protect patient privacy. The hospital found potentially inappropriate accesses to the medical records beginning no later than 2013, and possibly much earlier.

Without technology in place to provide alerts when access to a medical record is inappropriate, the organization now has to notify every single patient they've encountered since 2013, which will probably end up being a very costly process.

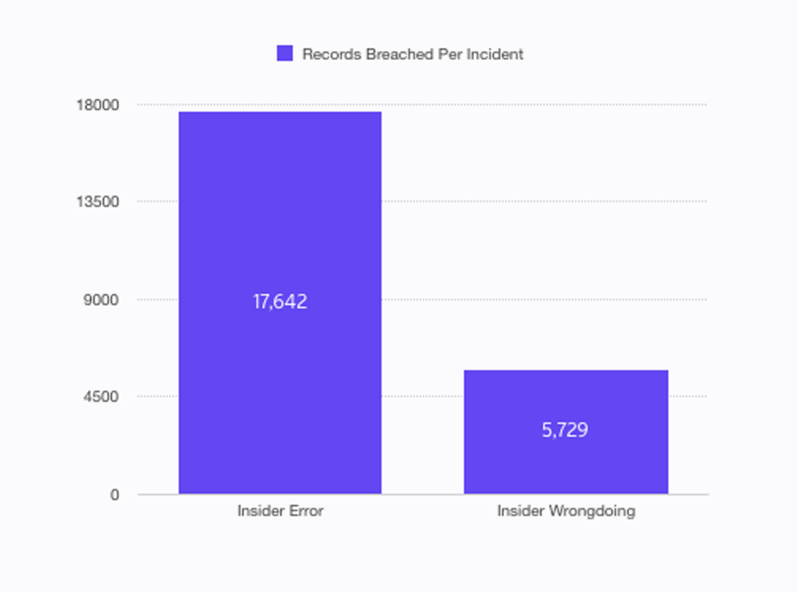

Figure 3a. Average Number of Patient Records Breached by Type of Insider Incidents

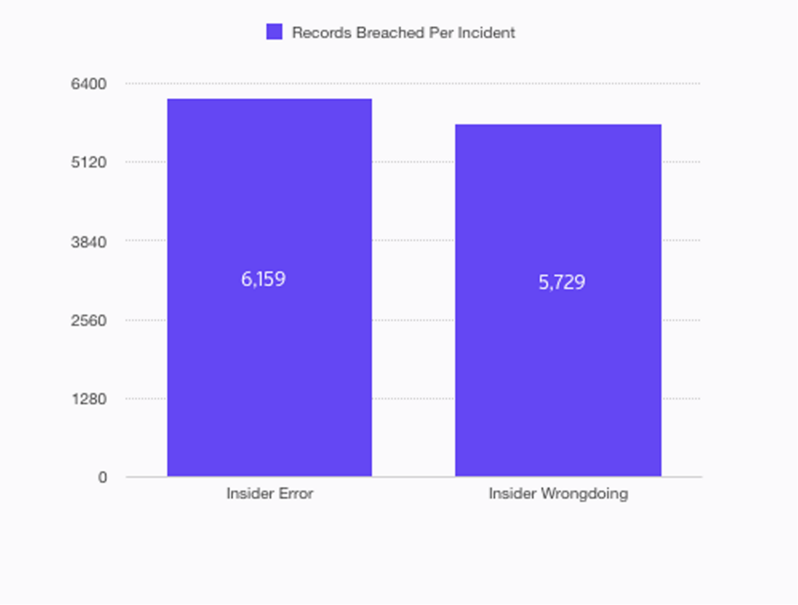

Figure 3b. Average Number of Patient Records Breached by Type of Insider Incident (Outliers Removed)

Hacking and Ransomware Responsible for 26.8% of all 2016 Health Data Breaches

Hacking and ransomware made headlines throughout the year as 2016 saw an explosion of ransomware cases across all sectors, with healthcare being no exception. Some entities chose to pay ransom demands to ensure patient care would not suffer any interruptions after doctors and personnel were unable to access files that had been encrypted. In one unfortunate case, patient data were irretrievably lost during recovery from backup, reminding us all of the need to not only maintain backups, but to test them periodically to ensure they will work in the event that they may become necessary.

In addition to cases of ransomware, we also saw non-ransomware cases where hackers acquired databases and subsequently tried to extort covered entities. When extortion failed, they put patient databases up for sale on the dark web. There were so many patient records put up for sale in 2016 that the price per record dropped significantly as the market became flooded.

For the 120 hacking incidents included in our analyses, we had the number of records affected for 99 incidents; those 99 incidents resulted in a staggering 23,695,069 breached records, or 87% of all patient records included in the analyses. Those 120 incidents included 30 incidents in which we know that ransomware was involved, and 10 incidents that involved ransom or extortion demands but not ransomware. The 120 reports do not include any incidents involving the newer type of ransomware that wipes files, as those hacks were not disclosed until after our cutoff date for inclusion in this analysis.

Given the number of ransomware cases this year, it may seem surprising that there were only 30 cases disclosed. We suspect that the 30 cases are a significant underestimate due, in part, to at least two factors. First, HHS's public breach tool only codes incidents as "hacking" but does not provide any information as to whether a hack involved ransomware. Second, many entities did not realize that they should be reporting these incidents until July, when HHS issued guidance on whether ransomware incidents are to be reported as breaches under HIPAA (see sections 6-8). Until then, entities may well have thought that they didn't need to report their breach.

Insider Threat vs. External Threat - What Will 2017 Bring?

While hacking accounted for the majority of patient records breached in 2016, insider incidents resulted in a larger number of breach incidents (120 vs. 192 respectively). We predict that 2017 will be the Year of Insider Breach Awareness, with organizations realizing that this constant and significant problem has gone unaddressed for too long, with the focus for the last couple of years being more about catching up on external threats.

While a smaller proportion of total records breached, the sheer number of insider breaches, and the disproportionately great impact they can have on patients' lives and a hospital's bottom line means that we must be particularly wary of insider threats. In a real-world example, a hospital employee shared details of an adolescent's attempted suicide with people at his school. The child was bullied and made fun of by his peers, resulting in his mother suing the responsible healthcare organization. This type of small-scale breach greatly affected the patient's life and could end up costing the hospital significantly in legal fees, fines, and settlement. In addition, as our nation's health systems become increasingly digitized and interconnected, we face an ever-more dangerous landscape of individuals who have some level of legitimate access to patient data, and could readily abuse that access with malicious intent.

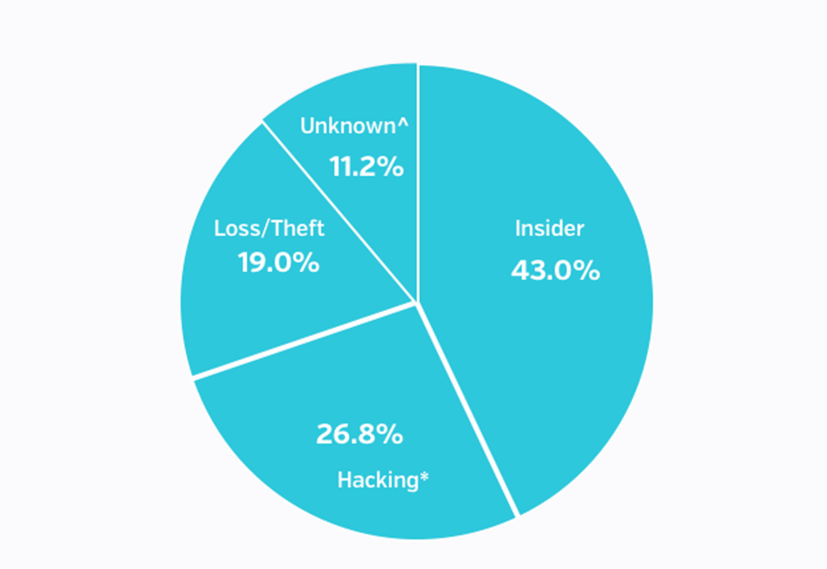

Figure 4. Types of Incidents, 2016 Health Data Breaches[3],[4][5]

Types of Entities Reporting

Of the 450 reported incidents in 2016, 356 incidents involved healthcare providers (80% of reported entities), followed by 45 incidents involving health plans.

28 of the 450 incidents (6.3%) were reported by business associates or third parties. While this number seems small, it's important to note that 131 (29%) of the 450 total incidents involved a business associate or third party, affecting at least 17,170,488 patient records. As Figure 5 shows, BA/vendors seemed to have been involved in almost every type of health data breach reported in 2016. Numbers were available for 112 of these BA-related incidents. An alert from US-CERT, while not specific to health data, offers a number of useful recommendations to better protect data. Covered entities

[3] *Also includes ransomware and malware incidents

[4] ^ Includes incidents reported in HHS's breach tool where there was insufficient information to categorize the incident

[5] Figure 4 percentages are determined from 447 incidents.

should consider whether their potential business associate or vendor adheres to these recommendations to protect patient data.

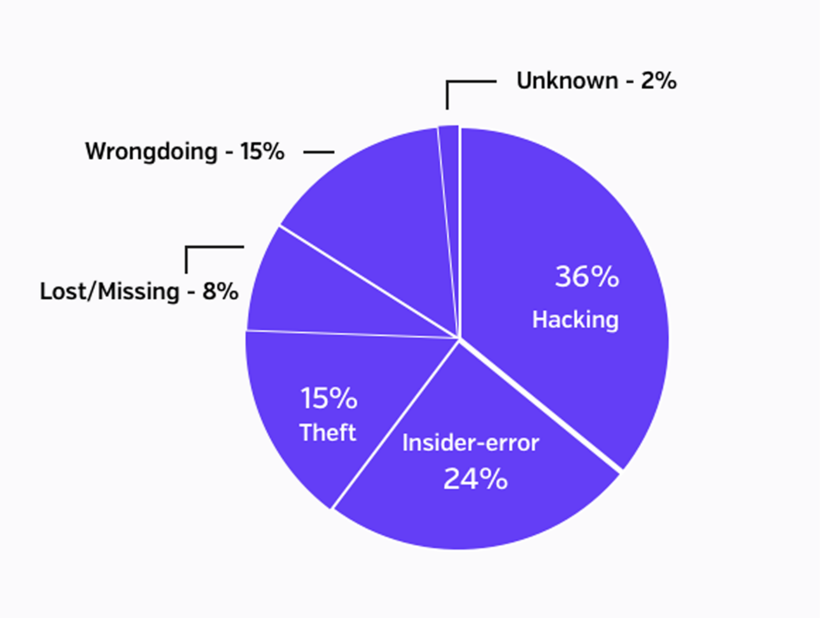

Figure 5. Business Associate/Third Party Involvement in Health Data Breaches, 2016

It is worth noting that, even in our digital age, paper records were involved in 86 incidents. There may be more, but some reports were lacking the detail that would have enabled that determination. The largest paper incident involved more than 450,000 patient records that fell or blew off a truck during transportation to a facility for secure destruction.

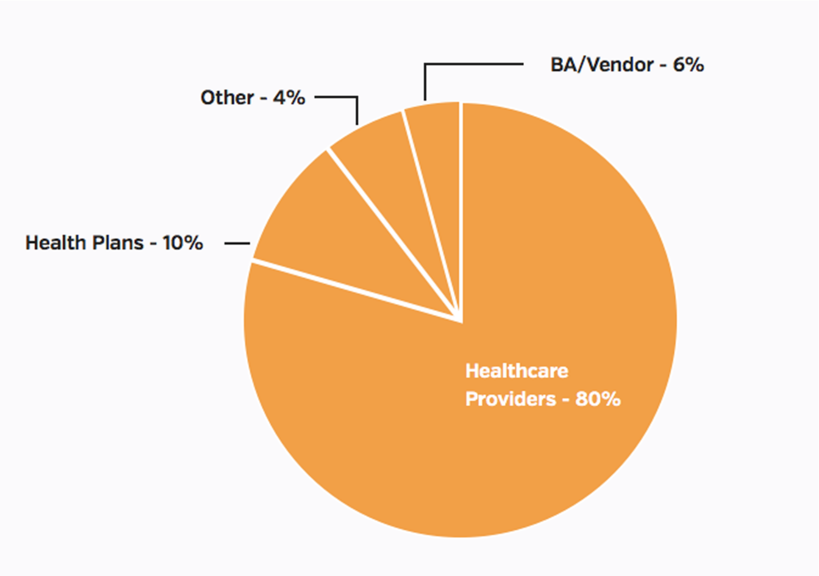

Figure 6. Types of Entities Reporting, 2016 Health Data Breaches

Health Data Breaches Take 233 Days to Discover, and 344 Days to Report

Of the 142 incidents reported in 2016 for which we have data, it took an average of 233 days for a healthcare organization to discover they had a health data breach. Perhaps most troubling is that the time to discovery specifically in cases of insider wrongdoing was more than double that - 607 days. There are many reasons why it can take an organization so long to discover a breach has occurred. Limited budgets and resources can be to blame — not all organizations will be able to detect breaches in an automated and precise manner. If organizations only have one or two employees dedicated to finding “red flags,” it will take significant time to weed through the noise and accurately detect the violations. Another reason is that many organizations have taken a reactive approach to privacy monitoring, only worrying about breaches to patient data once they are brought to their attention by the affected party, allowing for inappropriate access to the patient data to go unnoticed for extended periods of time, if it is detected at all. Entities may also be alerted to breaches by outside sources like the media.

It took an average of 344 days from the time the breach occurred to when HHS was notified. Please note that in some cases, long intervals may be due to law enforcement asking entities not to publicly disclose the breach, as to not interfere with current investigations or prosecution.   However it is important to remember that HHS requires entities to report their breach within 60 days of breach discovery. 86 reporting entities reported their breach to HHS within the 60-day time frame.

It goes without saying that it is essential for organizations to be proactive when monitoring patient data. The sooner a breach is detected, the quicker the healthcare organization can mitigate the risk of significant damage being done with their patients' data. The longer PHI is exposed, the more it can cost the healthcare organization and ultimately become increasingly troublesome for the patients.

State Frequency

47 states (94%) are represented in the 443 incidents for which we had location data. For three states, we did not find any disclosed breaches: Idaho, Vermont, and North Dakota. California had 73 incidents, which is the most reports of any state in U.S. Please note that numbers for some states are inflated because the analysis uses the state where the BA/vendor is located, not where the client is located.

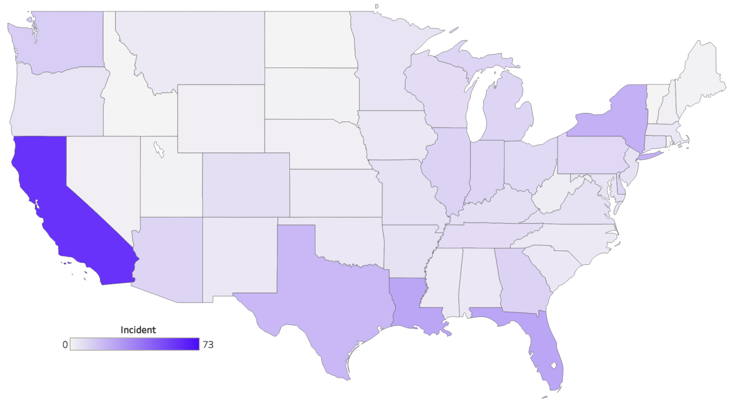

Figure 7. Number of Health Data Breaches by State, 2016

Conclusion

As 2016 has drawn to a close and we look ahead to what 2017 has in store for health data security, the healthcare industry can make strides to change the breach landscape. This year's data has shown that the frequency of breaches has been steady and will continue to be until health data security becomes a top priority for healthcare organizations. This data shows that external or internal bad actors are not being deterred from wreaking havoc on healthcare organizations and their patients. 2017 will continue to see this level, or even greater levels, of health data breaches if healthcare organizations don't take steps to reduce their risk.

Insiders are a very real risk to the security of patient data. The high number of breach incidents, and the fact that these small-scale breaches can often go undetected, make these breaches especially devastating. The healthcare industry should prepare for an increase in insider health data breaches until organizations further require additional training and utilize technology to detect inappropriate accesses to the medical record, further reducing their breach risk.

Health data protection needs to be a top priority for healthcare organizations - keeping their institution out of the headlines, limiting financial impact, and increasing their patients' trust and satisfaction. While it can take only minutes to gain access to a patient's medical records, it can take months to detect a breach, and years to recover.

Critically, healthcare must move beyond thinking about privacy, security or compliance alone - these are merely three pillars of our true goal: ensuring trust. As an industry, we must think about the fundamental shifts we can effect to build and maintain this trust.

**

About Protenus, Inc.

Protenus is a proactive patient privacy analytics platform that protects patient data in the EHR for some of the nation's top-ranked hospitals. Our advanced platform for alerting, forensics, and reporting replaces costly consulting services, ineffective and outdated rules engines and traditional compliance offerings. Using data science and machine learning, Protenus technology uniquely understands the clinical behavior of each user that is accessing patient data to determine the appropriateness of each action, elevating only true threats to patient privacy and health data security.

About DataBreaches.Net

DataBreaches.net is a web site devoted to reporting on data security breaches, their impact, and legislative developments relevant to protecting consumer and patient information. In addition to providing news aggregation from global sources, the site also features original investigative reporting and commentary by the site's owner, a healthcare professional and privacy advocate who writes pseudonymously as "Dissent."

Methodology

The purpose of this section is to explain decisions that were used to guide our analyses.

Sources

Incidents included in the analyses for this report were compiled for Protenus by DataBreaches.net, and include:

- Incidents reported to HHS between January 1, 2016 – December 31, 2016 that appear on their public breach tool. Incidents reported to HHS before December 31 that were not added to the breach tool in time have not been included.

- Incidents that were reported to other federal or state regulators such as SEC filings or state-mandated notification to state attorneys general or consumer protection agencies;

- Incidents from covered entities affecting less than 500 patients if those reports were publicly revealed;

- Publicly disclosed incidents involving U.S. organizations or entities that are not HIPAA-covered entities but that involved what would be considered protected health information under HIPAA;

- Incidents based on research by DataBreaches.net that may not have been reported to federal or state regulators.

As a result of our broader approach to investigating breaches that put protected health information at risk, this report includes the 315 incidents on HHS's breach tool plus an additional 135 incidents, for a total of 450 in our sample.

Coding

In addition to going beyond HHS's public breach tool to find breach incidents, this report also uses significantly different coding and analysis than HHS's public breach tool, permitting analyses that are not readily conducted based on HHS's tool, as follows:

- HHS's "unauthorized access/disclosure" category was abandoned in favor of a more refined analysis that allowed us to do a deeper dive into the rate and scope of insider/human error breaches vs. insider/intentional wrongdoing breaches.

- HHS's "Hacking/IT incident" led to further analysis of incidents reported in that category to determine if there was actually an external attack or if – as was the case in a number of incidents – entities were reporting being "hacked" when it might be more accurate to describe the incident as an unintended exposure of PHI on public FTP servers that researchers or others then accessed. In those cases, regardless of how the entity submitted the incident to HHS, our analysis coded those incidents as "inside – error," just as failures to restore firewalls after an upgrade that resulted in data acquisition were coded as "insider-error."

Calculating Time to Reporting

The inclusion of numerous third-party incidents resulted in the decision that for purposes of determining time intervals for "date of breach to date of discovery" and "date of discovery to date of public report," we would define the "discovery date" as the date that the third party first discovered the breach, and not the date that they first informed the covered entity about it.

In calculating time intervals between date of breach and date of public report, we defined the date of public report as the date that the entity first reported the incident to HHS or a regulator, or the date that there was a media report or something like a Twitter announcement that made the public aware that there had been an incident.

In some cases, we did not have exact dates, but only knew the month or year the breach first occurred. In calculating the interval between the breach to discovery and between the breach and reporting:

- If data was only available for the month or year of the breach, the first day of the year or month was used for calculation purposes.
- The date a BA/vendor first discovered the breach was used as the discovery date and not the date the covered entity first learned of the breach.

State Data

For state frequency data, if a Business Associate or vendor was responsible for the breach, we assigned the breach to the state where the BA or vendor is headquartered or located, if the third party's identity was known. In cases where the third party's location could not be determined, the incident was assigned to the covered entity's state.

Any inquiries about the data collection or analyses should be directed to kira@protenus.com.

Disclaimer

This report is made available for educational purposes only and "as-is." Although we have tried to provide accurate information, as new information or details become available, any findings or opinions in this paper may change. Despite our diligent efforts, we remain convinced that the breaches we find out about publicly are only the tip of a very, very large iceberg, and any patterns we see in publicly disclosed breaches may not mirror what goes on beneath the tip.