BREACH BAROMETER REPORT: MID-YEAR REVIEW

2017 on Track to Exceed 2016 Trend of 'One Health Data Breach Per Day'

–Protenus, Inc. in Collaboration with DataBreaches.net

Introduction

The first half of 2017 has not shown healthcare any mercy, with health data breaches continuing to plague the industry. The trend first noted in our 2016 year in review continues well into 2017, with averages of at least one health data breach per day. Based on the new report from the Identity Threat Resource Center (ITRC), healthcare comprises 30% of all U.S. data breaches, coming in second only to the business sector. Our findings, in addition to the ITRC report, should serve as a call-to-action for healthcare organizations to learn from these unfortunate experiences and increase efforts to thwart inappropriate access to their patients' most sensitive data.

Findings for First Half of 2017

From January to June 2017, there were a total of 233 breach incidents reported to HHS, the media, or state attorneys general. Our previous reports for January - May have been updated for this mid-year report as more information became available, so totals reported here may not correspond exactly to prior Breach Barometer reports for specific months.

For the 193 incidents for which we had numbers, 3,159,236 patient records were affected. As Figure 1 shows, the number of breach incidents each month were relatively consistent except for a spike in June. June has been the worst month so far in terms of total number of breach incidents (52 separate incidents), while March was the worst month in terms of the number of affected patient records, as seen in Figure 2. The largest single incident so far in 2017 for which we had numbers involved 697,800 patient records, and was the result of insider-wrongdoing. Other incidents may have involved even larger numbers of patient records, but we did not have definite numbers for every incident to use in our analyses.

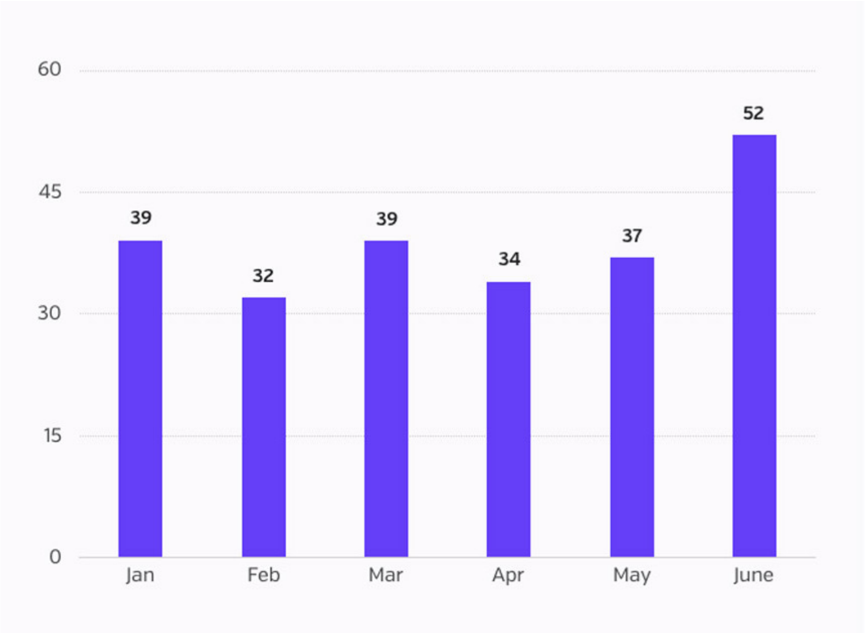

Figure 1. 2017 INCIDENTS INVOLVING PHI OR MEDICAL/HEALTH INFORMATION

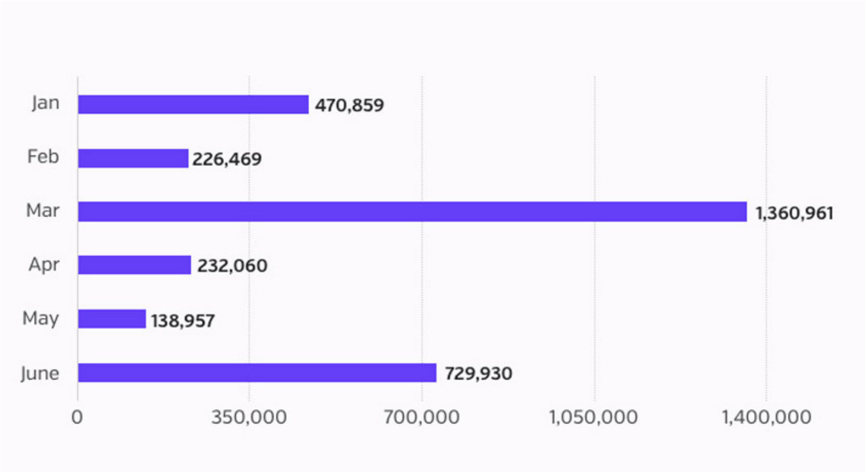

Figure 2. 2017 NUMBER OF BREACHED PATIENT RECORDS

Insider Threats Remain Constant

41% of the health data breaches so far in 2017 (96 incidents) were a result of insiders. For the 73 incidents for which we have detailed information, 1,166,674 patient records were affected. The number of breach incidents and affected patient records is on course to meet or exceed the findings for 2016. For the purposes 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 or patient privacy.

57 of the 96 insider incidents disclosed this year were a result of an insider-error or accident, while 36 incidents were a result of wrongdoing. In three cases, there was insufficient information to determine whether the incidents should be coded as error or wrongdoing. While there were substantially more breach incidents that involved insider-error (57 incidents vs. 36 incidents), it was insider-wrongdoing that affected considerably more patient records (423,009 vs. 743,665). Insiders with malicious intent can cause significant damage due to the simple fact that their inappropriate access isn't immediately detected because they have legitimate access to the EHR. It's important for healthcare organizations to ensure their employees are well trained on appropriate use of their EHR access and remind them of the potential repercussions of negligent or malicious behavior.

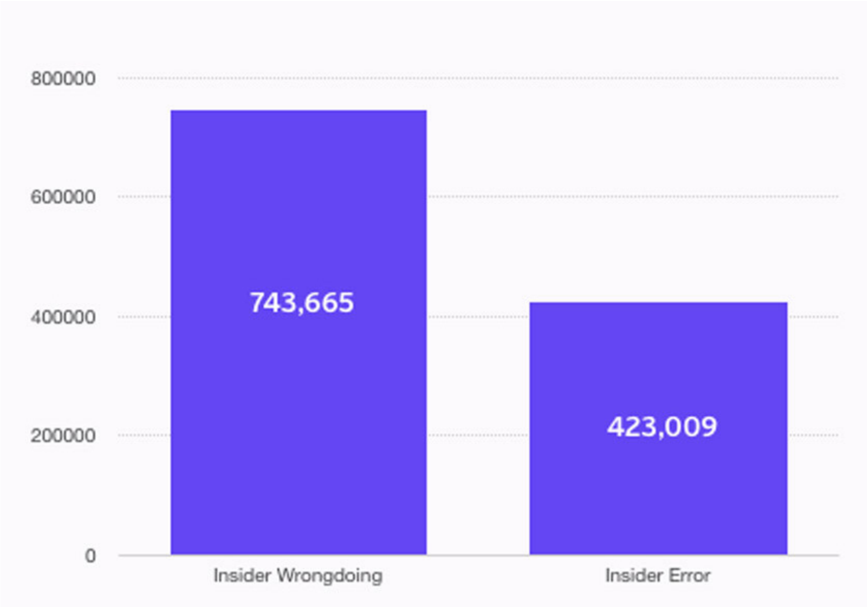

Figure 3. NUMBER OF PATIENT RECORDS BREACHED BY TYPE OF INSIDER INCIDENT

Hacking Responsible for 53% of Breached Patient Records

Hacking (including ransomware incidents) still looms large in healthcare. So far in 2017, there have been 75 separate breach incidents that were the result of hacking. For the reported hacking incidents for which we have numbers, 1,684,904 patient records were affected. Ransomware or malware was specifically mentioned as involved in 29 of the hacking incidents, but we know that there were many more cases that involved hacking and/or malware that were simply reported as "hacking" or an "IT incident" per the HHS breach tool. And in many cases, Databreaches.net has found through independent research that incidents were not reported at all, it seems. Although we should expect to see higher numbers in 2017 due to HHS instructing entities to report ransomware attacks unless they can prove that data were not accessed or exfiltrated, ransomware attacks may continue to be under-reported and have potentially devastating effects. As with one example, three weeks after one entity was hit with Petya, its clients still cannot use its transcription service. In addition to transcription, 10 other products appear to be affected, including those used for radiology, billing and software that tracks quality of care.

BakerHostetler recently summarized advice for entities as to how to protect themselves from ransomware while Craig Musgrave of The Doctors Company offers additional suggestions. Others have provided discussion of WannaCry, Petya, and NotPetya. These discussions all emphasize that many of these attacks would be easily preventable, if only entities deployed good security hygiene and updated/patched promptly.

Other types of external attacks also appear to be under-reported or unreported. As one example, earlier this year we saw thousands of databases from all sectors wind up with their data removed or wiped out in attacks described as "ransacking." Only a few of those incidents were ever reported to HHS, leaving us to wonder how many databases storing PHI may have been removed by criminals who sought ransom, but the entities did not report the event because they believed that the data were just deleted, but not copied and exfiltrated.

In addition to what may be numerous incidents of "ransacking" that were never reported to HHS, according to the FBI, there are numerous incidents where PHI exposed on public FTP servers has been targeted by criminals, yet we have seen very few of those incidents appear on HHS's breach tool. DataBreaches.net has further details on these incidents.

In addition to under-reported ransomware attacks, ransack attacks, and exposed PHI on FTP servers, some victims of hacking and extortion attempts also do not appear to have reported their incidents to HHS. As we saw in 2016, the criminals known collectively as TheDarkOverlord continued to attack and attempt to extort entities in the healthcare sector. Those victims who did not agree to pay their demanded amount may have found their patient data dumped publicly by the annoyed attackers.

So far in 2017, TheDarkOverlord has revealed attacks on five entities in the healthcare sector, dumping patient data from three of them publicly. They also dumped patient data from two entities they had reported hacking last year. Of note, however, only a handful of those incidents have been reported to HHS. As DataBreaches.net discussed, it is not clear whether all of the entities are HIPAA-covered entities, but some of these incidents probably should have been reported to state regulators, and yet DataBreaches.net found no evidence that most of them were ever reported to states, either.

Worryingly, another threat actor has recently emerged who is also attacking healthcare entities and attempting to extort them. Like earlier reports by TheDarkOverlord, this other threat actor claims to exploit Remote Desktop Protocol (RDP) being left enabled by entities who not only fail to disable RDP but also generally use incredibly weak or easy-to-guess passwords.

“In the past year, I’ve spent countless hours interviewing TheDarkOverlord and other threat actors who attack the healthcare sector,” DataBreaches.net’s blogger, Dissent, tells Protenus. The more sensitive your information is, the greater the commercial value to an extortionist. If you don’t want your patients’ information being publicly dumped or sold on the darknet, update and patch your systems, regularly backup your data and don’t leave your backup connected to the internet, and teach and re-teach your employees not to click on links in emails. As a recent incident shows, phishing is still a serious risk. And Dissent adds, “And don’t forget to check - and change, if need be - the default settings on your storage systems and devices. There are way too many databases that are exposed to the world because rSync devices were not secured properly. Criminals know how to search to find unsecured backups with what is likely valuable information.”

The Human Impact of Health Data Breaches

According to DataBreaches.net, one of the worst hacking incidents in 2017 so far involved an outpatient private practice mental health center in Maine whose patient records were hacked and put up for sale. “Some of those patients are sex offenders,” DataBreaches.net told Protenus. “Others may be victims of sexual abuse. The patient records included notes about their therapy sessions that included references to other people in their lives, where both they and the other people might be identifiable by their initials and detailed descriptions. When I saw the sample record from the for sale listing, I felt sick inside," the blogger stated.

While the sale of more than 4,000 patients' sensitive mental health records is the stuff privacy and infosecurity nightmares are made of, the revelations of HIV status or other physical ailments may also lead to patients being stigmatized or experiencing problems.

In 2016, the criminal collective known as TheDarkOverlord revealed that they had hacked a dentistry practice in New York City, but that the practice would not pay their extortion demands. In a statement posted on a public paste site in October, the criminals wrote, in part (errors as in the original):

> *Being the good-natured people we are, we contacted the dentistry after we had a copy of their patient records safely in our possession. After notifying them of this fact, we then proposed a course of action that would accomodate (sic) us both. However, for reasons unknown, they suddenly became hostile towards us and using very colourful language, foolishly declined (pictured on Twitter). However, after much contemplation, we've come to the conclusion that they may not be the most situationally-aware people. We understand that they'll require a gentle nudge or two which is why we'll still be giving Aesthetic Dentistry a choise (sic) to cooperate with us or suffer a stabbing pain inflicted by yours truly.*
>
> *As proof that what we say is true, you will find below a link to sample of the data. Note that they contain PHI. Their records show that some patients have HIV, AIDS, Herpes Simplex, or Venereal Disease, and much more. More of these records specifically will be released if Aesthetic Dentistry does not cooperate with us.*

In May, after months of silence, TheDarkOverlord publicly dumped the database. As they had threatened, it included the patients' HIV status and other sensitive details. As disturbing as this hack and data dump may be, it never appeared on HHS's public breach tool - a timely reminder that we may not be seeing some of the worst breaches on the government's public breach tool.

Insider Threat vs. External Threat

While hacking has accounted for the majority of patient records breached, Figure 4 shows that insiders are responsible for 28% more breach incidents than hackers (75 vs. 96 incidents, respectively). The media generally gives more attention to hacking incidents (32% of total incidents), as they create a large splash when breaching a large amount of patient records in one incident, however, insider incidents can often go longer, even years, without detection creating much more devastation in its wake. Without advanced data analytics in place, it can be difficult for organizations to detect and understand what distinguishes normal user behavior within the EHR from abnormal behavior with malicious intent. We remain hopeful that 2017 will be the Year of Insider Breach Awareness as healthcare organizations continue to become increasingly aware of how detrimental the aftermath of a breach can be to both the organization's bottom line as well as their patients' lives and livelihoods. Early detection will be key to get ahead of these health data breaches; the sooner a breach can be detected, the sooner the organization can take necessary steps to mitigate its overall impact.

It's important to note that there were 34 reported incidents of patient records theft, and we have numbers for 33 incidents, affecting 107,437 patient records. There were also 7 incidents in which records were lost or missing, affecting 4,865 patient records. These incidents comprised 18% of total breach incidents so far in 2017. 9% of incidents were classified as unknown as there wasn't enough information to make a determination (Figure 5).

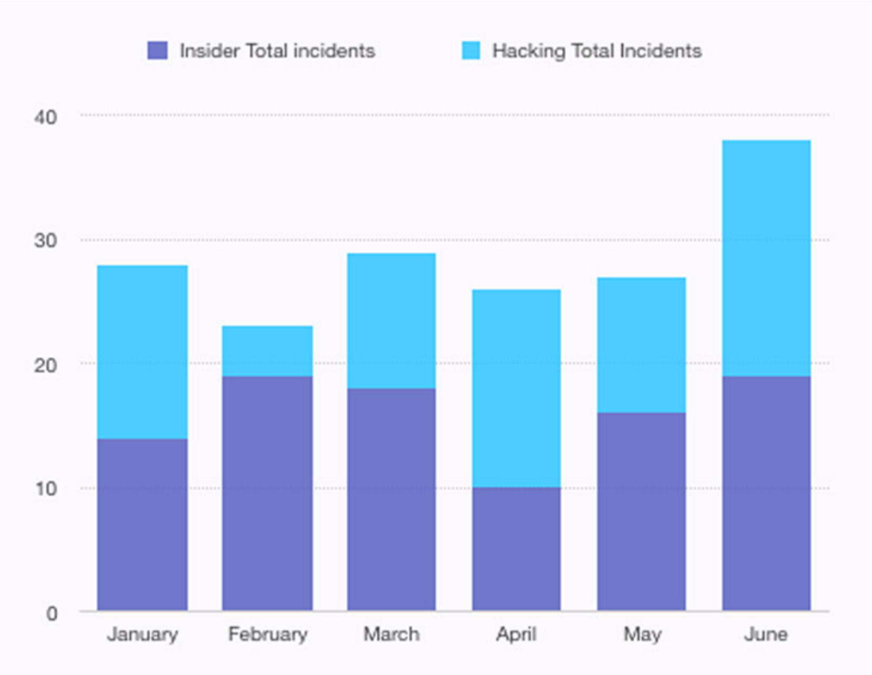

Figure 4. INSIDER VS. HACKING TOTAL INCIDENTS, 2017 HEALTH DATA BREACHES

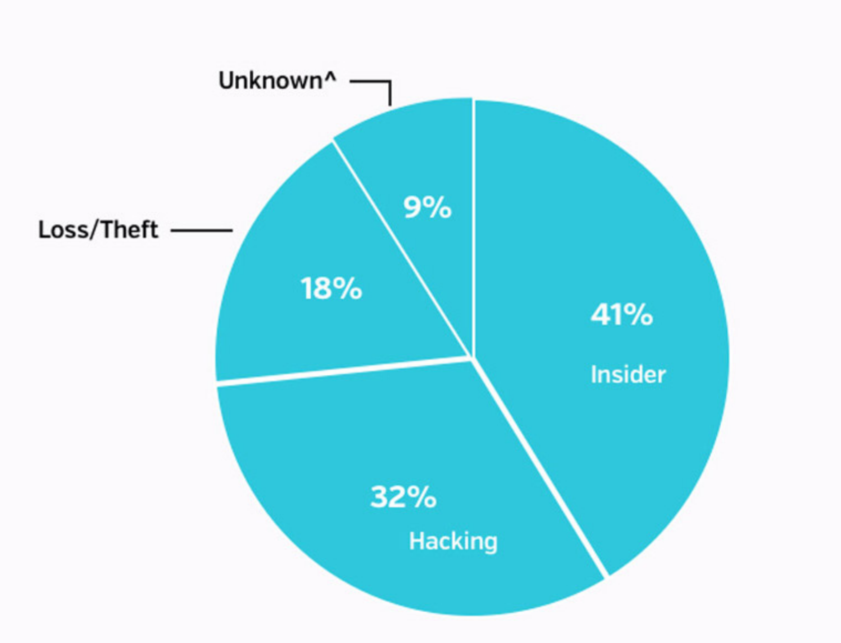

Figure 5. TYPES OF INCIDENTS, 2017 HEALTH DATA BREACHES

Types of Entities Involved in Health Data Breaches

Of the 233 health data breach incidents in Q1 and Q2 of 2017, 187 of those (80%) involved healthcare providers, 26 incidents involved health plans, and 14 incidents involved a business associate or third-party. There were also seven breach incidents that were categorized as miscellaneous or other, as these incidents didn't fall into one of the main categories used in our analyses. It should be noted that there could be more incidents involving third-parties but there was not enough information for a number of incidents to make that determination.

37 of the 233 incidents (16%) were reported by business associates or third parties. While this number seems small, breach incidents involving BA or third parties has affected 892,066 patient records. Also, these incidents are already 32% higher than the total number of incidents involving BA or third parties reported in 2016. Healthcare organizations need to focus on educating and training their internal employees but also need to have key systems in place to ensure the business associates that work within their system are also diligent about protecting patient privacy, by performing activities like checking to ensure BAs have FTP servers configured correctly and have backups in place.

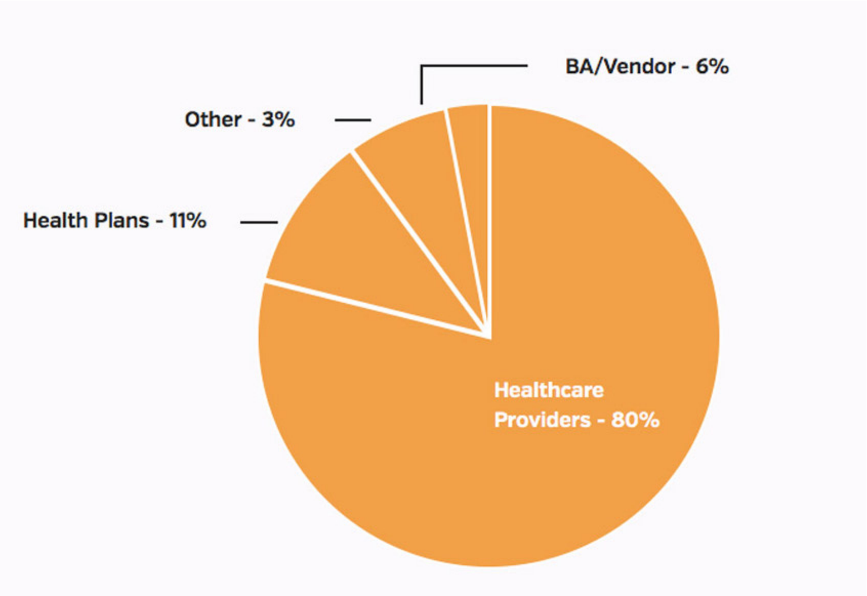

Figure 6. TYPES OF ENTITIES REPORTING, 2017 HEALTH DATA BREACHES

It is also worth noting that even in the era of digital records, there were 37 health data breach incidents that involved paper or film patient records. There may have been more incidents in which paper or film records were involved, but again, some reports were lacking detail that would have enabled that determination.

Great Improvement in Time to Report Breaches to HHS

Of the reported incidents for which we have numbers, it took an average of 325.6 days (median = 53 days) for healthcare organizations to discover a breach had occurred (Figure 7; Figure 8). The mean and median are drastically different given the extreme range of this data. Some entities discovered a breach immediately, while other incidents went undiscovered for years.

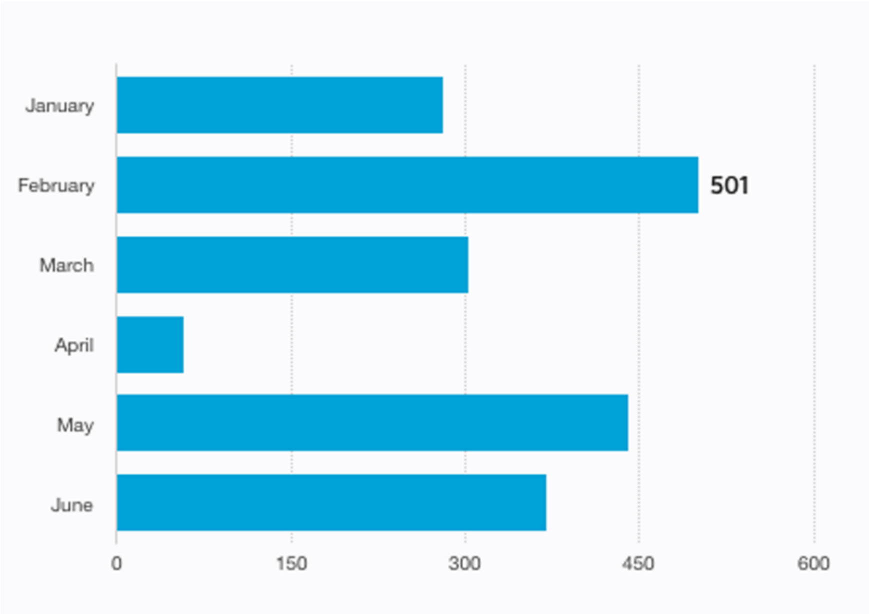

Figure 7. MEAN NUMBER OF DAYS TO BREACH DISCOVERY, 2017 HEALTH DATA BREACHES

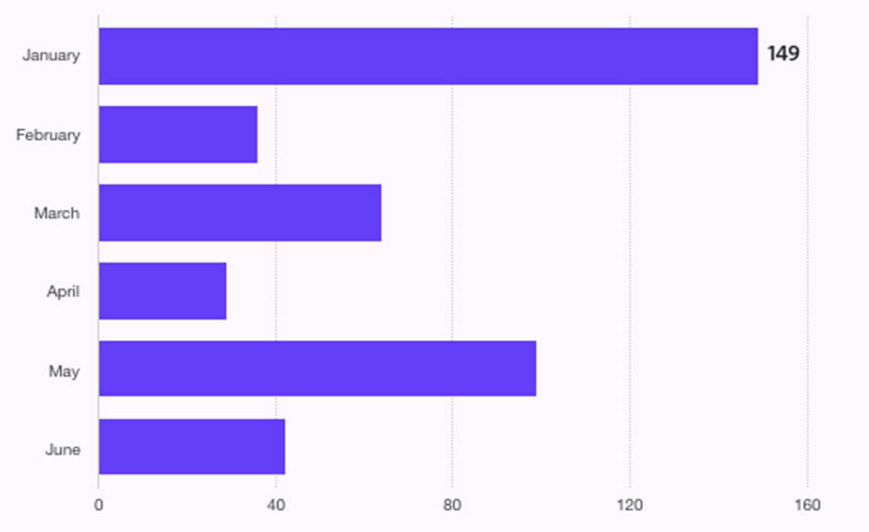

Figure 8. MEDIAN NUMBER OF DAYS TO BREACH DISCOVERY, 2017 HEALTH DATA BREACHES

It also took an average of 54.5 days (median = 57 days) from the time the breach was discovered to when it was reported to HHS (Figure 9; Figure 10). This is an impressive improvement from previous reports of organizations taking significant time to report to HHS. One can't help but acknowledge that HHS began fining organizations who did not report their breach within the mandated 60-day reporting window. Whatever the reason for improved reporting, it's a huge step in the right direction for healthcare to better understand the threats to their patient data, detect them, and report them quickly.

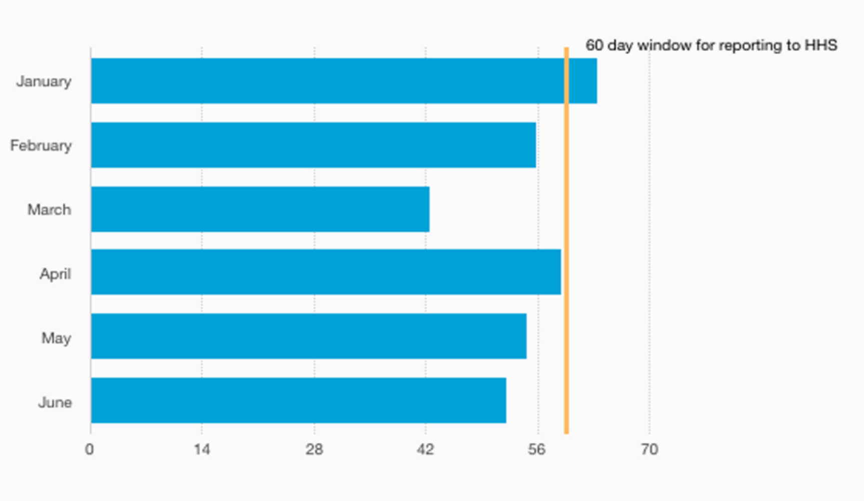

Figure 9. MEAN NUMBER OF DAYS FROM BREACH DISCOVERY TO HHS REPORTING, 2017 HEALTH DATA BREACHES

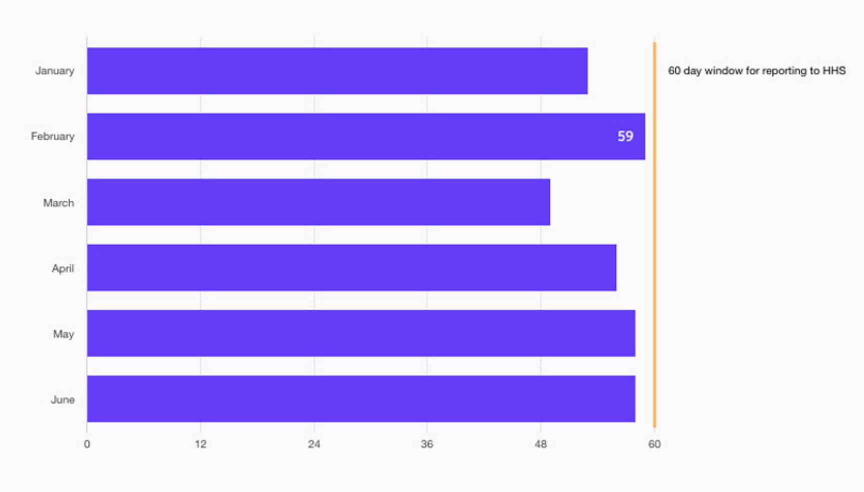

Figure 10. MEDIAN NUMBER OF DAYS FROM BREACH DISCOVERY TO HHS REPORTING, 2017 HEALTH DATA BREACHES

Breach Incidents By State

44 states are represented in the 233 health data breach incidents. California had 28 incidents, which is the most reports of any state. Texas followed closely with the second highest total of 22 separate health data breach incidents. It should be noted that California routinely has a relatively high number of breach incidents, but this could be due to higher reporting entity and patient volume, and/or more robust reporting. It should be noted that there as one breach incident in which the location of the breach incident could not be determined and therefore categorized as unknown.

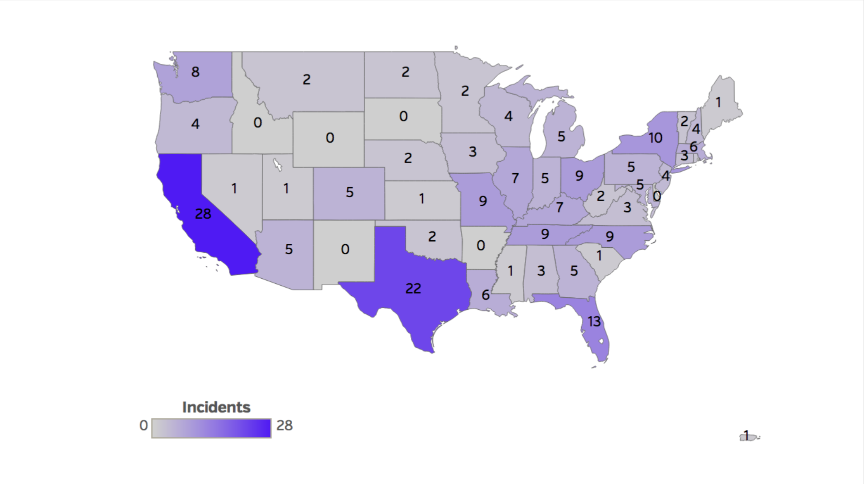

Figure 11. HEALTH DATA BREACHES BY STATE, 2017

Conclusion

The 2017 health data breach landscape seems to be consistent with the trends we first noticed in 2016. The data continue to show that external and internal bad actors are not being deterred from wreaking havoc on healthcare organizations and their patients. The time is over to bury our heads in the sand - we should learn from one another on steps that can be taken to reduce the overall risk of experiencing a breach, as well as openly discuss the industry's privacy and security shortfalls. Armed with this knowledge, we can better protect patient privacy and ensure patient trust when they are seeking healthcare at any of this country's healthcare organizations.

Health data protection needs to be a top priority for healthcare organizations - keeping their institution out of the headlines, limiting a breach's impact, and ultimately increasing patient trust in the organizations where they seek care. While it only take a few minutes to gain access to a patient's medical record, it can take months to detect such a breach, and years to recover from its aftermath.

Summary of Findings

1. Reporting health data breaches to HHS has improved, however detection is still dismal;

    1. 57 days, average time for healthcare organizations to report to HHS

    2. 325.6 days, average time for organizations to discover a breach had occurred

2. There is still evidence of significant unreported breaches and issues with centralized reporting;

3. Patterns show 2017 to be on track to worsen and surpass last year (2016) in terms of numbers of breach incidents and severity of attacks;

    1. 2016 total: 450 incidents vs. 2017 mid year total: 233 incidents

    2. 2016 total hacking: 120 incidents vs. 2017 mid year: 75 incidents

    3. 2016 total insider: 2M patient records vs. 2017 mid year: 1,166,674 patient records

4. Insiders are increasingly responsible for a significant amount of health data breaches, 28% more than hacking and ransomware;

    1. 2017 mid year insider breaches: 96 incidents

    2. 2017 mid year hacking events: 75 incidents

5. People's lives are being greatly affected by these breaches, far more then just an identity theft issue, very personal, sensitive information is being made public in a horrific way.

**

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 website 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, 2017 – June 30, 2017 that appear on their public breach tool.
- 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.

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 a 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.