White paper

Protected Health Information Data Breach Report

verizon

verizon

Contents

verizon

Introduction and methodology

Welcome to the latest edition of the Verizon Protected Health Information Data Breach Report (PHIDBR). The goal of this report is to inform security practitioners in the healthcare industry – and anyone else who has a level of responsibility for the protected health information (PHI) of their employees – about the threats that they face.

PHI data loss, and all of the pertinent regulations and disclosure requirements associated with it, is not solely the problem of the CISOs at healthcare organizations, but more on that later.

Let's start with some quick facts about this report and what they tell us about the issues that the healthcare industry as a whole needs to address:

- 58% of incidents involved insiders – healthcare is the only industry in which internal actors are the biggest threat to an organization.
- Medical device hacking may create media hype but the assets most often affected in breaches are databases and paper documents.
- Ransomware is the top malware variety by a wide margin. 70% of incidents involving malicious code were ransomware infections.
- Basic security measures are still not being implemented. Lost and stolen laptops with unencrypted PHI continue to be the cause of breach notifications.

We aim to inform using data we have analyzed from 1,368 security incidents. Security incidents where PHI was at risk, but not confirmed as compromised, are considered breaches in this report (1,292 in total). The extremely common scenario of a password-protected, but unencrypted laptop stolen from a medical professional's car is a prime example, as is a ransomware infection. We made the decision to also include all breaches for the healthcare industry, as PHI data loss is not the only infosec dragon you must slay if you are working in this arena.

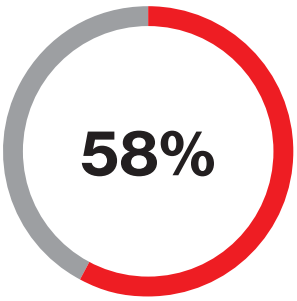
The threat actors, motivations, tactics and the assets ultimately affected will be discussed in detail to encourage a focus on the various efforts required when battling the most common threats associated with the healthcare industry and PHI.

About the data

The 1,368 incidents that underpin this report are a subset of the data behind our annual Data Breach Investigations Report (DBIR). Included in this report are incidents that meet one or more of the following requirements:

- The industry was healthcare[1]
- The data type disclosed or at risk was medical records
- The data subject victim relationship was patient

The timeframe begins where the maiden installment of this report ended – 2015. The dataset will include incidents from the 2016 and 2017 DBIRs. In addition, publicly disclosed events recorded in the Vocabulary for Event Recording and Incident Sharing (VERIS) Community Database (VCDB) up to November 2017 are also included. The disclosure requirements around PHI can be onerous, but a by-product is a rich, open-source well of data and we encourage all of you to learn more about VCDB at github.com/vz-risk/VCDB.



58% of incidents involved insiders – healthcare is the only industry in which internal actors are the biggest threat to an organization.

1. A more comprehensive list of organizations that would be categorized as healthcare can be found here: naics.com/six-digit-naics/?code=62

verizon

Definitions

Medical records

For the purposes of this study, we use the term “medical records” from the VERIS framework[2] to describe data that is medical in nature. This is not an exact synonym of PHI, which is identifiable back to a specific individual. A significant portion of the incidents within this dataset were collected as a result of required notifications, so we can infer that a significant amount would meet the definition of PHI and represents information collected from an individual, and covered under one of the state, federal or international data breach disclosure laws.

PHI

PHI may be collected or created by a healthcare provider, health plan, employer, healthcare clearing house or other entity. Per the defining criteria, data contained within a patient’s healthcare record is deemed to be PHI if there is a reasonable basis to believe the information could be used to identify an individual. In the US, the disclosure of this type of information would trigger a duty to report the breach under the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), and one or more state laws. Examples of identifiable data elements may include but (due to variances in the many federal, state or international regulations associated with PHI) are not limited to:

- Name, address (including just postal code), telephone and fax numbers
- Email addresses
- Medical insurance or Social Security/National Insurance numbers
- Any date more granular than year
- Information about named beneficiaries
- Any (financial or otherwise) account numbers, license, vehicle or certificate numbers
- (Medical or otherwise salient) device or serial numbers
- Any associated internet protocol (IP) addresses or URL/URIs
- All biometric data (for example finger, retinal or voice prints and/or DNA)
- Full facial photographic images or images that have unique identifying characteristics
- X-rays and diagnostic images

2. Learn more at veriscommunity.net

verizon

Victim demographics

Our dataset comprises incidents from 27 countries, albeit with a strong US bias to the data (almost three-quarters of incidents). Public access to the US Health and Human Services (HHS) incidents, as well as a significant number of records from the US Veterans' Administration (VA), contribute to this bias. The VCDB dataset focuses solely on publicly disclosed breaches, so countries with breach-disclosure laws are more likely to be represented in this report than are countries without such laws.

We stated this in our prior PHI report and it remains true today: "The US bias does not mean that this report isn't useful for organizations elsewhere in the world. Our data has consistently shown that adversary tactics are influenced by the data they are interested in, as well as the assets that process and store that data – not the country in which the data resides. Attack methods and human errors are not tied to latitude and longitude."

Healthcare is the predominant industry in this report (95% of incidents where industry was known) – which doesn't come as a surprise. It's certainly worth noting again that it isn't the only industry in this report – 60% of the NAICS industries listed below experienced breaches of PHI data. Health insurance organizations, billing services and courier services all handle PHI without acting as medical care providers. Organizations, regardless of industry, that process workers' compensation claims or manage employee wellness plans/health insurance programs all have to address security and privacy of PHI.

When the victim organization size is known, we have a 53%/47% breakout between large (over 1,000 employees) and small (1,000 or fewer employees) businesses. The result when looking solely at organizations in the healthcare industry is an almost exact 50/50 split between the two. It isn't just large, complex organizations that are vulnerable to data breaches. Small organizations such as doctor-owned clinics are also disclosing losses of PHI.

Industry (NAICS code)	Total	Small	Large	Unknown
Healthcare (62)	1,099	292	297	510
Public (92)	106	7	45	54
Retail (44–45)	56	16	30	10
Finance (52)	41	8	22	11
Educational (61)	25	5	10	10
Professional (54)	23	10	3	10
Other services (81)	10	3	2	5
Information (51)	9	4		5
Manufacturing (31–33)	8		6	2
Unknown	7			
Administrative (56)	4	2		2
Entertainment (71)	4	4		
Accommodation (72)	1	1		
Agriculture (11)				
Mining (21)				
Utilities (22)				
Construction (23)				
Trade (42)				
Transportation (48–49)				
Real estate (53)				
Management (55)				

Table 1. Incidents by industry and organization size

verizon

Threat actors and motives

One of the most interesting findings of this report and of the healthcare industry section in the 2017 DBIR is the threat actor breakout, or more simply stated "who is behind all of this?" Focusing on incidents where data was either confirmed as disclosed or was at risk, internal actors are more common than external – which is unique to the healthcare industry.

Actors

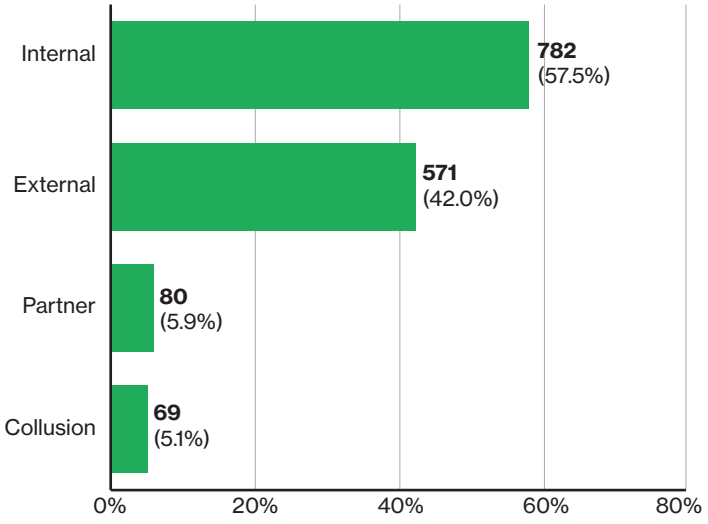


Figure 1. Threat actors within PHIDBR dataset, n=1,360

The healthcare industry relies on the timely and up-to-date accessibility of highly regulated data to a large percentage of employees. Would you prefer an ER physician fill out a request for your medical history in triplicate before initiating care, or intervene right away? The ability to access information quickly to allow a team of care providers to make point-of-care decisions is vital. Furthermore, in their defense, not all of these breaches were malicious in nature. Human error (which we will view more in-depth when we get to the threat actions section) is a causal factor in just over half of the breaches that featured an internal actor. This is evidenced by the significant number of breaches within the Internal portion of Table 2 with N/A as a motive. Unfortunately, (or fortunately, depending on one's point of view) when mistakes are made that put PHI at risk, they must be reported.

When there's an observable motive for a data breach, regardless of "whodunit," it's most often money. From a standpoint of internal actors, the access that healthcare workers have to personal information of patients affords a convenient means to commit fraud of various types (for example tax return fraud or opening lines of credit). Insiders are also frequently prone to curiosity, and the accessing of patient data outside of their job responsibilities is reflected in the 94 instances where fun is the motive behind the data breach. For example, the admission of a family member, acquaintance or well-known personality into a hospital can present a temptation for employees who have technical access to that patient's health record but no direct role in providing care or services to that patient. Any unwarranted access into that patient's record simply to appease their curiosity would be (and is) considered a breach. Lastly, convenience as a motive comes into the picture when insiders do something that will make it easier for them to get their work done, but as a consequence also puts data at risk. An example would be violating data handling policies by storing sensitive data on unapproved hardware.

Actor motives	Internal		External		Partner	
Financial	148	48%	338	90%	10	71%
Fun/curiosity	94	31%	16	4%	2	14%
Convenience	32	10%	–	–	2	14%
Grudge	14	4%	14	4%	–	–
Espionage	11	3%	6	2%	1	7%
All others	11	3%	6	2%	–	–
N/A	353		1		44	
Unknown	213		142		50	

Table 2. Threat actor motives within PHIDBR breaches, n=306, 375, 14

Threat actions and affected assets

We define actor tactics at a broad category level (e.g. Was malware used? Was a social engineering attack leveraged?) as well as more specific varieties of each category (e.g. ransomware or phishing). We traditionally see strong associations between threat actions taken and the assets that are affected. This isn't surprising since the shortest distance between two points is a straight line, but while perhaps not surprising, it can be enlightening.

In this section, we'll look at the threat action categories, the most common varieties of those actions and the assets that are most often affected as a result. This will bring to life several common breach scenarios. We focused on combinations of threat actions and assets commonly found within incidents. It's important to clarify that the actions didn't always directly affect the asset, but they're both present in the event chain. Note that none of these are mutually exclusive and it's normal for several threat action categories and multiple threat action varieties to be present in an incident or breach event chain, just as it's possible for a person to be suffering from more than one illness at once.

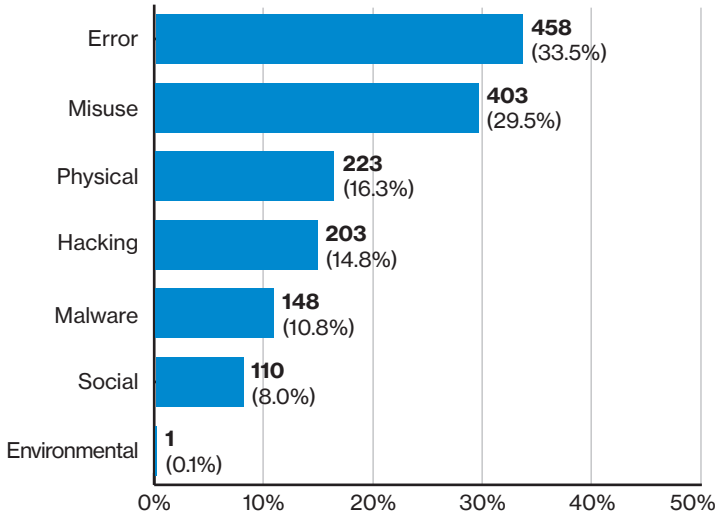
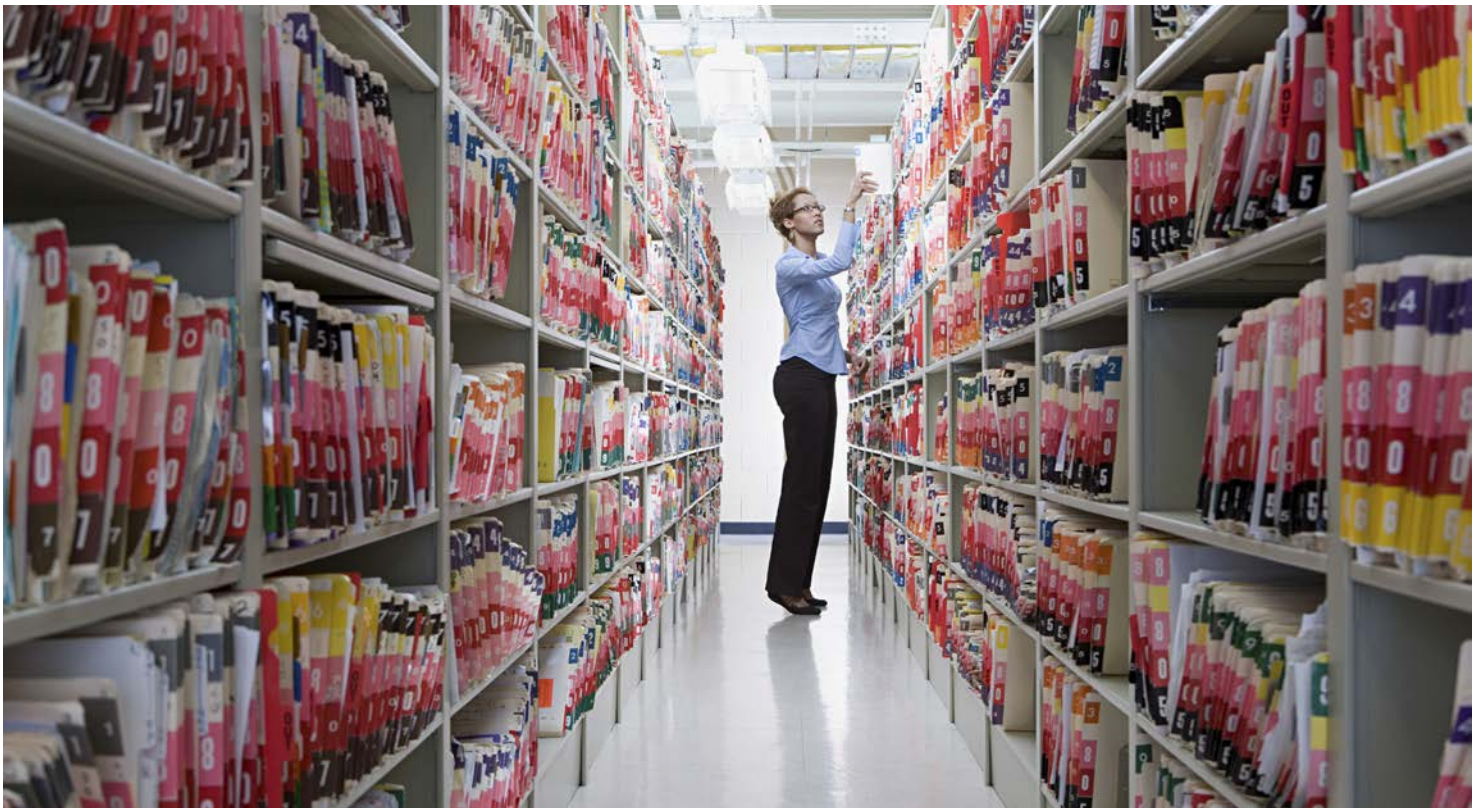


Figure 2. Threat action categories within PHIDBR dataset, n=1,368



verizon

Error

Incidents in which unintentional actions directly compromised an attribute of a security asset. This doesn't include lost devices, which are grouped with theft.

There is a tremendous amount of information flow in healthcare: prescription information sent from clinics to pharmacies, billing statements mailed, discharge papers physically handed to patients, copies of ID and insurance cards filed, and so on. Sensitive data meant for Person 1 inadvertently given to Person 2 is categorized as misdelivery, and is the most common type of error. Disposing of sensitive data in an insecure manner and the physical misplacement of assets follow. Rounding out the top 5 are publishing errors, which is the erroneous publishing of sensitive data on an asset with a wider-than-intended viewing audience, and misconfigurations. When we look at the most common combinations of action varieties and affected assets within incidents featuring human error, we gain additional context.

Healthcare has a paper problem. There has been much attention paid (and rightfully so) to electronic health records, but Table 3 shows that hard copy documents are the assets most often involved in incidents involving error. Sensitive data, including medical information in printed form is misdelivered, thrown away without shredding, and lost. The first ePHI combinations that we see involve the aforementioned publishing of sensitive data on public websites and misdelivery (again), this time via email.

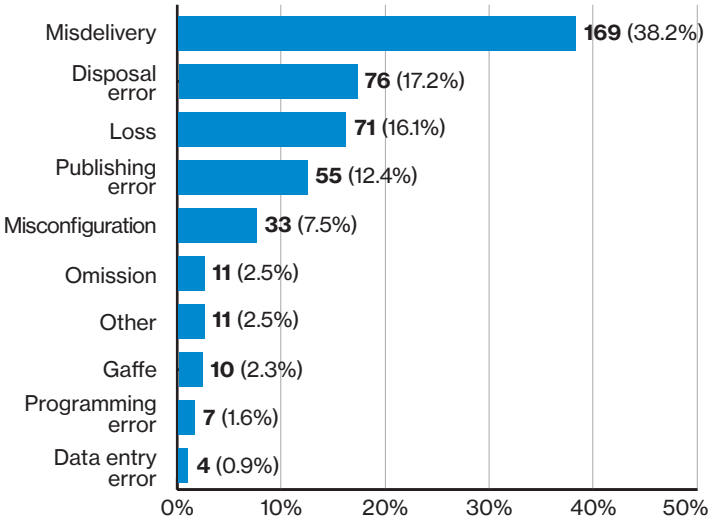


Figure 3. Top threat action varieties within Error, n=442

Threat action	Affected asset	Number of incidents within Error	Percent of incidents within Error
Misdelivery	Documents	90	20%
Disposal error	Documents	70	15%
Loss	Documents	36	8%
Publishing error	Web application	33	7%
Misdelivery	Desktop	32	7%
Loss	Flash drive	20	4%
Misconfiguration	Database	16	3%
Misdelivery	Unknown	16	3%
Misdelivery	Mail server	11	2%
Misconfiguration	Web application	9	2%

Table 3. Top combinations of Error varieties and affected assets

verizon

Misuse

Incidents involving unapproved or malicious use of organizational resources. These mainly involve insider-only misuse, but outsiders (due to collusion) and partners (granted privileges) are included as well.

Unlike the unintentional and motiveless errors we're all capable of making, actions in the Misuse category require having a distinct motive. Those motives can range from the inappropriate (convenience) to the quite malicious (financial, grudge and espionage). Regardless of the motivation of the actor, over 80% of incidents are comprised of people simply utilizing established logical (privilege abuse 66%) or physical (possession abuse 17%) access to sensitive data in an unauthorized manner.

As discussed previously, access to a great deal of sensitive information is necessary for healthcare professionals to successfully carry out their duties. But along with that access comes the relatively easy ability to abuse it. Privilege abuse occurs when a person uses logical access to databases without having a legitimate medical or business need to do so. Possession abuse is similar, but is misusing physical access to data. What they do from there depends largely on what their motivation might be. Simple curiosity about a friend, acquaintance or family member can lead someone to access files they shouldn't view, but so can a desire to gain financially via identity theft or a wish to damage someone's reputation by revealing sensitive health-related information.

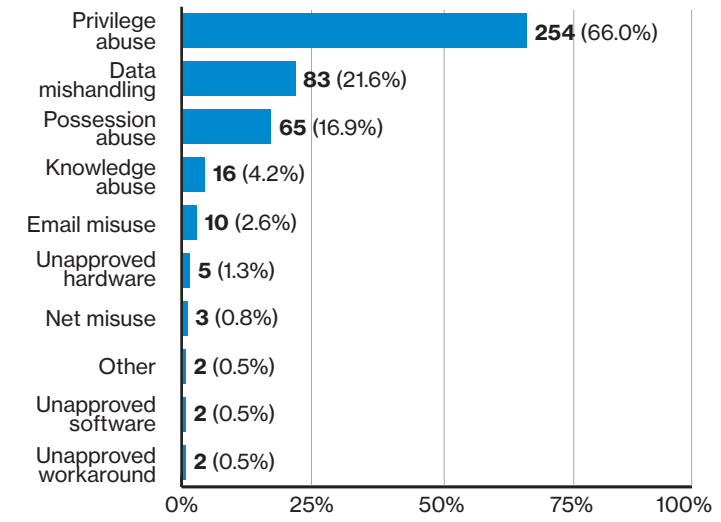


Figure 4. Top threat action varieties within Misuse, n=385

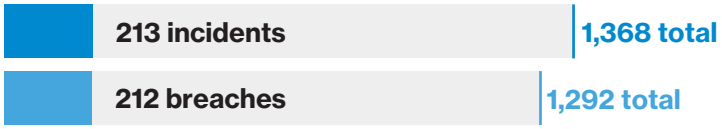
Threat action	Affected asset	Number of incidents within Misuse	Percent of incidents within Misuse
Privilege abuse	Database	200	50%
Data mishandling	Database	24	6%
Privilege abuse	Unknown	21	5%
Possession abuse	Web application	18	4%
Data mishandling	Unknown	18	4%
Possession abuse	Payment card	15	4%

Table 4. Top combinations of Misuse varieties and affected assets

verizon

Physical

Any incident where an information asset went missing, whether through misplacement or malice.



The Physical action type is exactly what it sounds like, when someone has physical access to an asset and uses that access to do something they shouldn't. By far the most common variety of physical actions is theft. Laptops account for the majority of theft for obvious reasons – their portability, and the fact that they can be repurposed for personal use or sold quite readily for cash, makes them an ideal target. In 47% of cases, the laptops were taken from the victims' own cars (where they frequently were left in plain view – and also often in clear violation of a policy stating that it shouldn't be there). An additional one-third of laptops were stolen from offices and other victim work areas. Theft has (and will) always occur, and we are all familiar with the basic concepts of avoiding it so there is no need to dig deeply into that subject here.

However, another thing that can be relatively easily and cheaply done to mitigate the impact of asset theft is full disk encryption. These days most laptops come with this capability built in to both Windows (BitLocker) and Mac (FileVault). Implementation is relatively simple and free, and consists of a few minor steps. Having a policy of centralized distribution of such mobile devices can ensure that they're handed over to employees already encrypted. While this will not replace the laptop, cover the cost of losing it, or regain the data lost, it will effectively render the information on the device totally useless to the criminal for fraud or any other purpose. This can also mean that disclosure is not required. Of course, you cannot encrypt paper documents and they account for the second most frequently occurring type of theft, whether taken from offices (44%) or employee's personal vehicles (29%). The remainder of theft consists of items such as disk drives, flash drives, payment cards and the occasional clunky desktop.

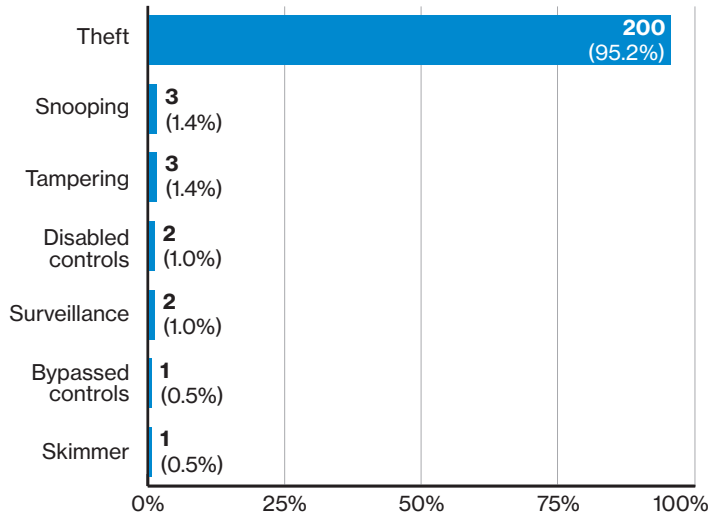


Figure 5. Threat action varieties within Physical, n=210

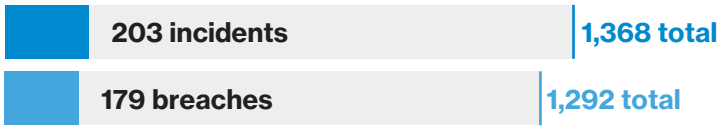
Threat action	Affected asset	Number of incidents within Physical	Percent of incidents within Physical
Theft	Laptop	94	44%
Theft	Documents	67	31%
Theft	Disk drive	12	6%
Theft	Payment card	12	6%
Theft	Flash drive	6	3%
Theft	Desktop	6	3%

Table 5. Top combinations of Physical varieties and affected assets

verizon

Hacking

Incidents where a threat actor gains unauthorized access to a victim's device or system. These attacks could use brute force, stolen credentials or backdoor/C2.



We have discussed how insiders blunder, lose things and otherwise behave poorly with regard to your PHI, and how local criminals enjoy the occasional smash and grab technique for their own profit. Now let us turn to those who don't have the luxury of having a desk inside the organization, or enjoy geographical proximity like those mentioned above, but must gain access from afar. Sometimes hacking isn't as easy as television commercials make it appear, and that's why it's always preferable for the criminal to use legitimate credentials to gain entry whenever possible – it makes their job simpler and helps to provide them cover while stealing data.

Therefore, the top two hacking varieties make a great deal of sense. Use of stolen creds and brute force are two sides of the same coin and are both geared toward getting your username and password. As stated earlier, threat actions aren't mutually exclusive and the person asset in Table 6 wasn't hacked. They were however tricked into providing credentials that often were used to access web-based email and thus have the association with the use of stolen credentials[3]. Unfortunately, most of the notifications only provided a high-level description of what happened, but not the specific hacking tactics that were used.

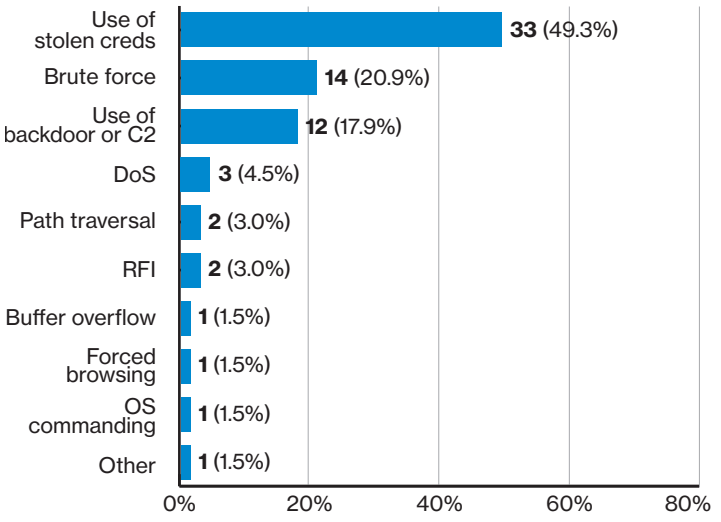


Figure 6. Threat action varieties within Hacking, n=67

Threat action	Affected asset	Number of incidents within Hacking	Percent of incidents within Hacking
Use of stolen creds	Mail server	18	9%
Use of stolen creds	Person (Unknown)	11	5%
Brute force	POS terminal	9	4%
Brute force	POS controller	8	4%
Use of stolen creds	Database	7	3%
Use of stolen creds	Database	7	3%
Use of backdoor or C2	Desktop	7	3%

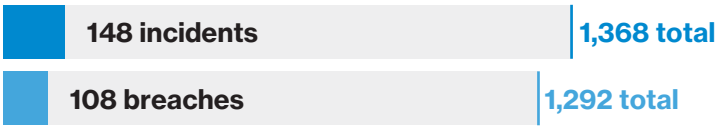
Table 6. Top combinations of Hacking varieties and affected assets

3. We'll see this scenario come to light in the Social action section as well.

verizon

Malware

Malicious software that enables an attacker to gain access to systems and data. Malware attacks are often opportunistic and financially motivated.



Malware is another way that attackers can damage healthcare organizations and illegally access PHI data. Although it can (and does) come in many forms, as Figure 7 shows, discerning criminals seem to prefer ransomware especially when it comes to attacks aimed at the healthcare vertical. Ransomware, as the name implies, is used to encrypt the victim's data, and then requires them to pay a fee or ransom to regain access to it. And it's absolutely endemic in healthcare, accounting for over 70% of all malware seen. Other common malware varieties such as RAM scrapers, backdoors and keyloggers are dwarfed by ransomware. Due to HHS regulations, ransomware outbreaks are to be treated as breaches (rather than data at risk) for reporting purposes. That poses the question: is it that healthcare organizations are doing a poor job of preventing ransomware attacks or does it only appear that way because they are required to report them all and other industries aren't? The answer is probably a little bit of both – it's only fair to point out that ransomware accounts for a very large percentage of malware in other industries as well. It's quick, requires very little effort on the part of the attacker, with low risk to the criminal, and is very lucrative.

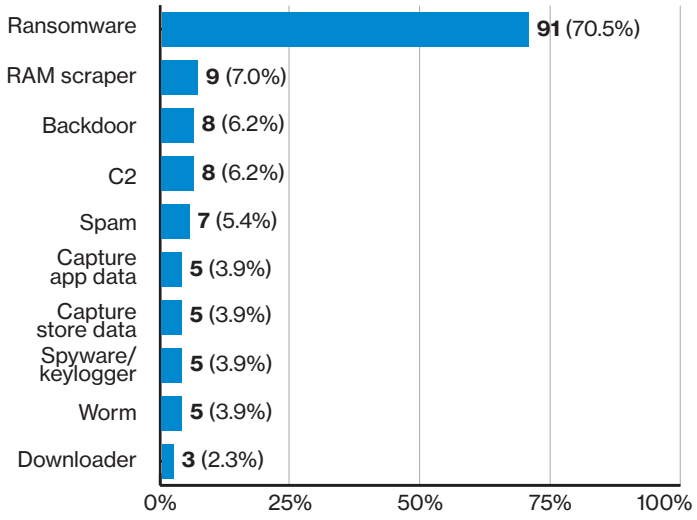


Figure 7. Threat action varieties within Malware, n=129

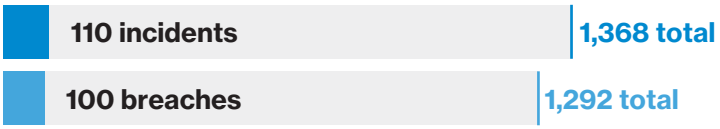
Threat action	Affected asset	Number of incidents within Malware	Percent of incidents within Malware
Ransomware	Database	29	20%
Ransomware	Unknown	21	14%
Ransomware	Server (Unknown)	16	11%
Ransomware	Desktop	15	10%
RAM scraper	POS controller	9	6%
RAM scraper	POS terminal	8	5%
Ransomware	Person (Unknown)	6	4%
Ransomware	File server	6	4%
Ransomware	End-user	5	3%
Ransomware	Web application	5	3%
C2	Desktop	5	3%
Ransomware	Laptop	5	3%

Table 7. Top combinations of Malware varieties and affected assets

verizon

Social

Incidents in which threat actors target people directly to try and gain access to their data and systems. This can involve the use of anything from a false URL to an email attachment.



Social attacks target what is sometimes jokingly referred to as the carbon layer of security – namely people. While any organization's people can be (and often are) its most valuable asset, from a security point of view they can just as frequently be its weakest link. Figure 8 shows that by far the most common type of action variety is phishing, followed by pretexting. Phishing is when someone sends a communication – most often via email to an individual attempting to influence them to open a malicious file or click on a link. If they take the bait, that leads to the compromise of non-human assets detailed in Table 8.

Phishing taken to the next level becomes known as pretexting. That's when the criminal emails, calls or otherwise engages an employee in a conversation with end goals such as duping the employee into providing them with their username and password or other sensitive data, or to get them to approve a fraudulent ACH transfer. They can pretend to be from a helpdesk, a superior, coworker or a partner business. Their pretext will be dependent on which of the recipient's strings they want to pull.

The other social attack that's found in the top combinations is bribery or solicitation. This is, when known, how we can track if an external group influences an employee to act as a mole on their behalf.

The healthcare sector includes some instances of collusion (when multiple types of actors work in concert to steal data). Usually, this is external and internal actors working together, but partner actors can also be leveraged.

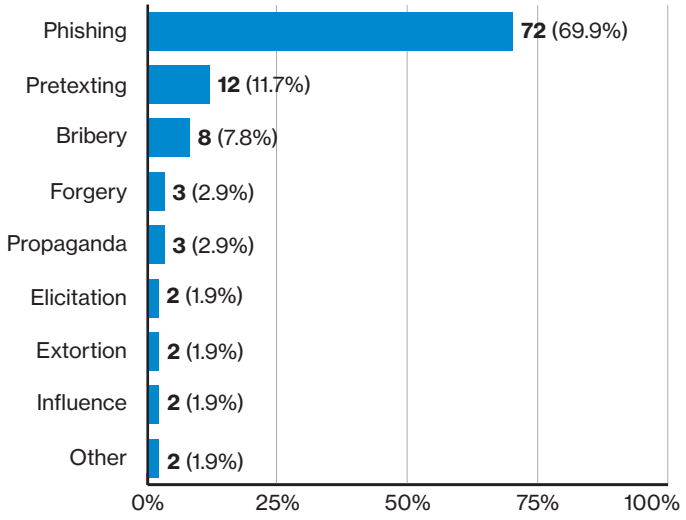


Figure 8. Threat action varieties within Social, n=103

Threat action	Affected asset	Number of incidents within Social	Percent of incidents within Social
Phishing	Person (Unknown)	46	42%
Phishing	Mail server	24	22%
Phishing	Desktop	21	20%
Phishing	End-user	17	19%
Bribery	Database	7	15%
Phishing	Web application	7	15%
Bribery	End-user	6	6%
Pretexting	Person (Finance)	6	5%
Phishing	Database	6	5%
Phishing	Laptop	6	5%

Table 8. Top combinations of Social varieties and affected assets

verizon

Data types

Earlier we listed a non-inclusive list of data elements that can be classified as PHI. Many of these elements group together into broader data types. The following VERIS data types were disclosed as a result of the incidents that comprise this report[4].

Medical records
Likely what first comes to mind when one thinks of a PHI breach includes, but is not limited to, diagnosis information, lab results, treatment plans, etc. Again, our breach data doesn't always provide enough information to define with certainty the ability to determine the patient identity along with the medical data. We are confident based on the data sources, and the other aspects of the breach that the majority of data defined as medical records would meet the requirements to be considered PHI.

Personal or PII
Personally identifiable information (e.g. Social Security/National Insurance numbers, name, date of birth)

Payment or PCI
Payment card information

Credentials
Usernames and passwords or other authentication tokens. While not PHI in and of itself, compromised credentials often are utilized to ultimately compromise additional data types.

Figure 9 reveals some interesting stories about the various data types. Starting with how often each data type is found in breaches within the PHI DBR dataset. Medical records are – as we would expect – the most common, and, along with personal information, are more likely to be compromised in larger numbers than PCI or credentials. These records are compromised at rest and are stored in bulk – whether in databases or resident on laptops, or even paper records that are lost or stolen.

The data indicates credentials aren't being compromised in large quantities, but stolen one at a time via social engineering, information stealing malware or simply guessed. PCI data in this dataset is most often compromised in small quantities by internal actors as opposed to captured in mega-breaches, but the distribution shown below does expose that larger hauls of PCI data aren't outside the realm of feasibility.

Overall data types disclosed

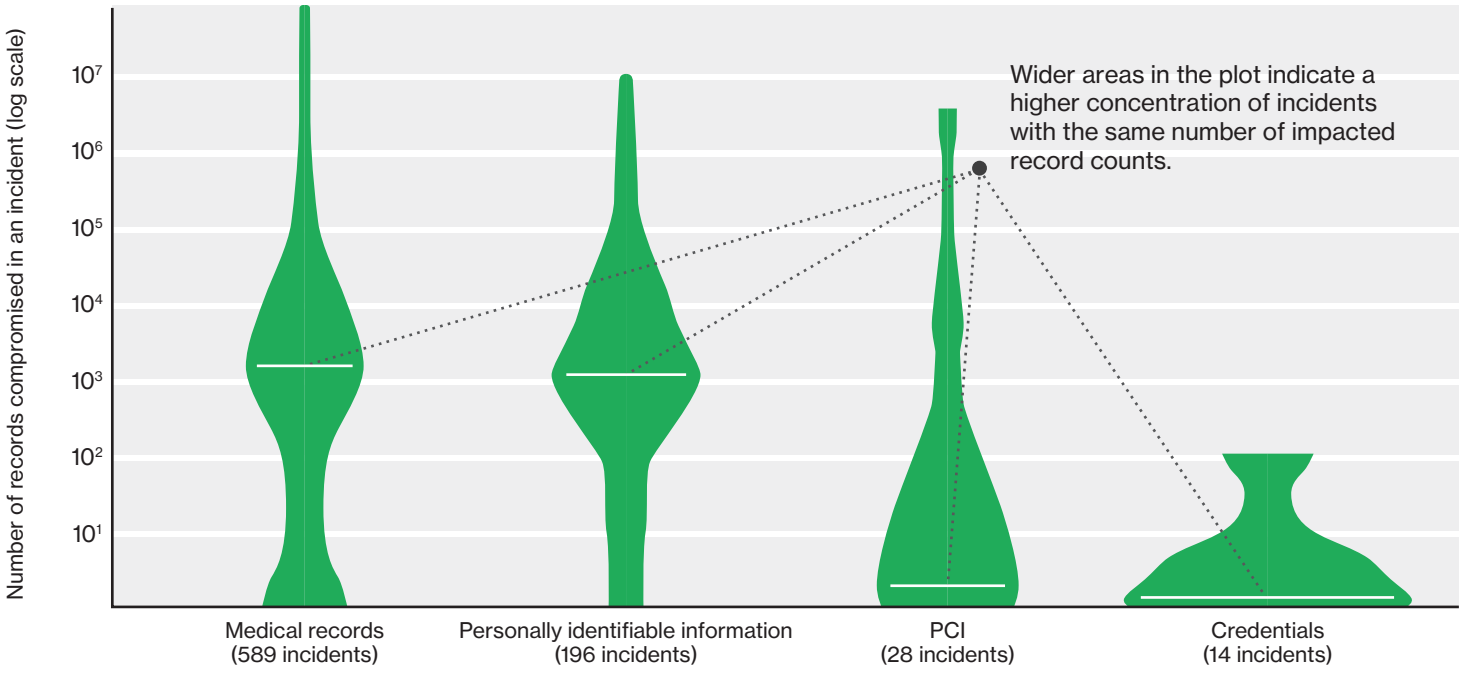


Figure 9. Data types disclosed

4. Other data types, such as banking information and sensitive internal data was also disclosed, but not with enough frequency to include in this section.

Healthcare NAICS breakout

In this section, we take a look at the Actions to see what kinds of incidents were experienced by the organizations in each of the three-digit NAICS codes. We could easily get stuck in the minutia here, so what follows is a breakout of the threat action categories per sub-industry and some interesting factoids we were able to pull out of the data when we focused on specific tactics.

When analyzing the specific tactics found within the top threat actions (Misuse, Error, Physical) nothing interesting was unearthed for errors and physical actions. We did find a couple of data points worth talking about in the area of Misuse, however. The majority of the incidents involving misuse were from clinics/offices (621) and hospitals (622). Most of these incidents involve the general abuse of privileges by staff. One interesting outlier was that the use of unapproved hardware was found in higher concentration in NAICS 621. This variety of misuse was over 12 times more likely to be found in this sub-industry than the rest of the dataset. We also found that a motive of espionage was six times more likely to be associated with clinics/offices than the rest of the population. These actions together describe a familiar chain of events starting with the use of USB drives to exfiltrate proprietary information for use after leaving an organization, either to move to a competitor or to launch your own practice.

Another contrast regarding Misuse incidents for clinics versus hospitals is how they're discovered. Incidents involving hospitals (622) are almost equally discovered by internal methods and external parties, but clinics are close to a 3:1 ratio of external to internal. Another noteworthy item is that hospitals were over eight times more likely to discover an incident via an IT review than the other victims. These reviews can be as simple as cross-referencing accesses to patient records and comparing them to dates of visits and/or whether they were in the direct care of the employee.

Nursing and healthcare facilities and social assistance victims were smaller sample sizes, but when comparing incidents of misuse of NAICS 623 strong associations to PCI data were uncovered. Physical payment cards were much more likely to be associated with these organizations than others. This is a product of physical access to patients' personal items while in their care and the illicit use of them for fraudulent purchases.

The healthcare industry is divided into four separate top-level NAICS codes:

- 621: Ambulatory healthcare services (includes all types of doctor and dentist offices)
- 622: Hospitals
- 623: Nursing and residential care facilities
- 624: Social assistance

Incident actions by industry

Figure 10. Actions by three-digit NAICS code

Timeline and discovery

Certain types of incidents found in significant amounts in this dataset don't add value when analyzing time-to-discovery metrics. Employees self-reporting lost or stolen devices are one example, a second being notification via a banner informing an organization that they are yet another ransomware victim. Those discovery methods are close to automatic and there is little we can do from a detective control standpoint to lessen those durations. The end result from filtering out those specific cases was a drop in the incidents discovered in hours and is displayed on the right.

The elephant in the figures is the number of incidents where the discovery was measured in months or years. A trip back into the dataset shows that half (51%) were employees misusing privileges. Once the inappropriate actions were discovered, often the behavior can be traced back for several years. A surprising finding was that the motives, when known, were more likely to be financial in nature as opposed to fun or curiosity. We would have expected a motive that isn't identifiable via financial fraud detection would have been more prevalent.

Discovery time

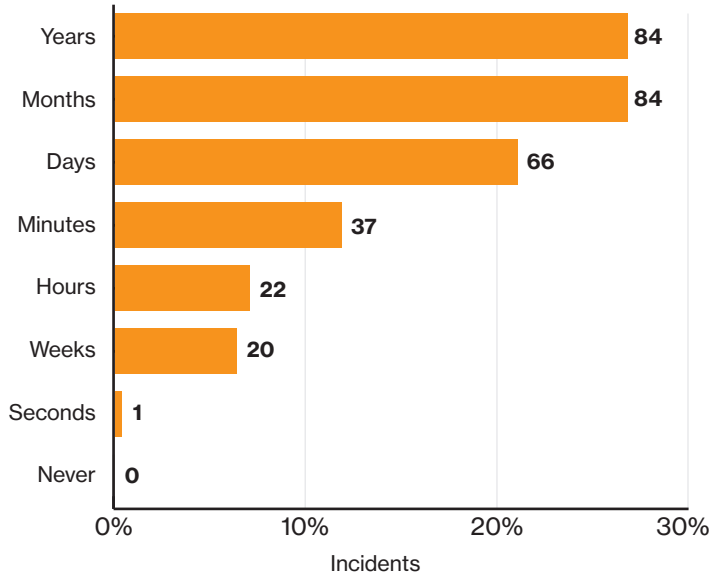


Figure 11. Time to discover (selected incidents), n=314

verizon

Wrap up

So, after taking a look at the data and analyzing the picture it paints, what can we take away from it? Are we viewing The Scream by Edward Munch? Or a peaceful alpine meadow by Bob Ross? It likely depends on your current role, responsibilities and recent experience handling PHI-related events.

While it's true that adequately protecting your organization from all the various avenues attackers can take to harm you can be onerous and challenging, there's plenty of room for hope. Some of the most common threat actions such as theft and loss (while expensive and irksome) aren't unique to the healthcare industry and many straightforward and non-technical approaches exist to combat them.

Additionally, one of the primary value adds of this report is that it's based on analysis of real-world events. That means that it illuminates some of the main trouble spots you're likely to encounter and being forewarned is forearmed. Knowing the areas of greatest concern allows an entity to dedicate more of its resources to address those concerns and to some extent mitigate the risk associated with them.

We have extracted numerous commonalities within incidents and breaches that have victimized the healthcare industry. And there are long-term strategic recommendations that we recommend as well as some tactical quick-wins that should be implemented as soon as feasible.

ePHI must be protected, but to not embrace a shift to an electronic healthcare record system because of a perceived increase in susceptibility to PHI loss isn't supported by our data. Modernization of record storage and data flows brings a new threat landscape, but the amount of breaches associated with old-fashioned paper documents is eye-opening. Work towards a reduction of paper-based PHI in your environment. Establish a holistic risk management program that protects not only ePHI, but also other sensitive data that's stored and processed by your organization. PCI data, internal procedural documents and employee PII. all must be taken into consideration.

Recognizing that strict restrictions to patient information can affect the ability to make timely and proper point-of-care decisions, there are improvements that can be made in the area of logical access controls to PHI. A comprehensive review and ongoing audits of access rights to sensitive data to ensure ease of access to front-line medical providers, yet reduce authorization creep within organizations is essential. There will always be a balancing act that healthcare security officers must face, but there's room for reduction of attack surface and internal threat.

As all industries move towards utilization of the Internet of Things (IoT), establishing a proactive policy of building security into any and all implementations is vital to getting ahead of what could be an increasing threat in the future. A formalized policy specific to testing and vetting of connected medical devices as well as third-party legal reviews of contracts should be developed. Focusing on resiliency and availability in regards to IoT implementations as well as integrity or confidentiality is important. Tabletop exercises and planning around environmental threats (severe power outages, natural disasters) or device malfunctions to ensure that backup plans exist to continue to treat patients should be planned and conducted.

An overall incident response (IR) plan should be established and include both internal stakeholders as well as external partners in areas of legal guidance and forensic investigative assistance. The ability to react quickly and efficiently can often make a difference in the level of impact an incident has on an organization. Just as with the IoT scenario, tabletop exercises and walk-throughs must be conducted to gauge the ability to execute what has been documented.

To initiate IR procedures and checklists, the discovery of a breach must occur. Improvements in detection of potential security incidents and/or data breaches are a core component of the overall risk management program. Validate your implementation of basic security fundamentals as we continue to see data breaches that have simple and cheap corrective actions associated with them. Then focus on more advanced detection and response capabilities.

Below are several short-term improvements that would directly address common threat actions highlighted in this report.

Full Disk Encryption (FDE)

FDE provides an effective and relatively low-cost method of keeping sensitive data out of the hands of criminals. FDE can also mitigate the consequences of physical theft of assets by limiting exposure to fines and reporting requirements. While this recommendation is straight out of a HIPAA Security Rule checklist, our data indicates it bears repeating here. Laptops are constantly stolen or lost with inadequate protections. Reduce your risk footprint where you can.

Routine monitoring of record access

Ensure that policies and procedures are in place which mandate monitoring of internal PHI accesses. Make all employees aware via security training and warning banners that if they view any patient data without a legitimate business need, there's potential for corrective actions. Deter employees from acting on motives of curiosity or financial gain.

Build resiliency to combat ransomware attacks

Obviously preventive controls regarding defending against malware installation are key. In addition to trying to prevent malware from entering your environment, steps should be taken to reduce the impact that ransomware can have against your network. Our data shows that the most common vectors of malware are via email and malicious websites. Don't allow a patient zero end-user device to easily propagate and spread ransomware to more critical assets and don't use devices with high availability requirements to surf the internet or receive external email. In May 2017, ransomware attacks in Europe brought several hospitals to their knees[5]. Make sure you include this in your IR scenarios and have plans in place that enable your staff to continue to function while the recovery takes place in the event that controls designed to limit the spread of infection are circumvented.

5. http://www.bbc.com/news/health-39899646

verizonenterprise.com