DBIR INDUSTRY SNAPSHOT: HEALTHCARE

A study conducted by the Verizon RISK Team with cooperation from the Australian Federal Police, Dutch National High Tech Crime Unit, Irish Reporting & Information Security Service, Police Central e-Crime Unit, and United States Secret Service.

DATA BREACH INVESTIGATIONS REPORT

A study conducted by the Verizon RISK Team with cooperation from the Australian Federal Police,
Dutch National High Tech Crime Unit, Irish Reporting & Information Security Service,
Police Central e-Crime Unit, and United States Secret Service.

Verizon's annual Data Breach Investigations Report (DBIR)[1] analyzes forensic evidence to uncover how sensitive data is stolen from organizations, who's stealing it, why they're doing it, how the victims responded, and what might have been done to prevent it. This Industry Snapshot draws information from the DBIR data set, but gives highlights focused exclusively on approximately 60 confirmed data breaches over the last two years within the Healthcare and Social Assistance industry[2]. Additionally, we reference the much larger collection of publicly-reported incidents in this sector[3] as a way to offer extended scope and contrast.

As with the annual DBIRs, the findings in this Snapshot are arranged using the Vocabulary for Event Recording and Incident Sharing (VERIS)[4] framework and based on breaches investigated by Verizon's RISK Team or one of our partner organizations, which include the Australian Federal Police, Dutch National High Tech Crime Unit, Irish Reporting and Information Security Service, Police Central e-Crime Unit, and United States Secret Service. Also like the DBIRs, all incidents in this snapshot involved confirmed unauthorized access and exfiltration of non-public information rather than potential exposures and other data-at-risk events.

DBIR INDUSTRY SNAPSHOT: HEALTHCARE

SUMMARY OF FINDINGS

Adopted in February 2010, the Health Information Technology for Economic and Clinical Health (HITECH) Act was created in part to motivate the healthcare industry to implement electronic methods to manage and more effectively share medical records. The act included a provision requiring covered entities to report data breaches of more than 500 records to the individuals affected, media outlets, and the Secretary of Health and Human Services. Since that time, the number of publicly-reported breaches in the healthcare vertical has understandably spiked. This upward trend, however, has not been as dramatic within our DBIR dataset, though the proportion of Healthcare incidents did hit a high mark (7% of incidents overall) in our most recent report.

The majority of attackers seek information from which they can directly or indirectly profit, including personal and payment information.

While blackmailing patients and hacking pacemakers are common hand-waving examples used by some to stress the importance of protecting medical records, the actual threat landscape is much more in line with run-of-the-mill cybercrime seen in other industries. The vast majority of attackers seek information from which they can directly or indirectly profit. This includes personal and payment information (including patient health and insurance data) used to supply organized criminal groups with what they need for all manner of fraudulent schemes.

This leads to two common patterns we see repeated throughout healthcare breaches: 1) attackers targeting point of sale (POS) systems and other assets in the payment chain, or 2) the physical theft and loss of devices (from which we may assume the value of the hardware is the intent). While protecting medical devices and records is a critical part of operating in the healthcare industry, organizations cannot lose sight of other assets being targeted by attackers.

1 To learn more about the DBIR series, visit verizon.com/enterprise/dbir.
2 We use the North American Industry Classification System (NAICS) to classify victim organizations. Descriptions of this and other industry groups can be found at census.gov/cgi-bin/sssd/naics/naicsrch?chart=2012.
3 As an example of publicly-reported healthcare breaches, see the list compiled by the U.S. Department of Health and Human Services: hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html.
4 For more information on VERIS or any of the classifications used in this report, see veriscommunity.net.

VICTIM DEMOGRAPHICS

Aside from their Healthcare industry commonality, the most notable characteristic of the organizations in this sample set relates to size.

Most organizations experiencing breaches within the Healthcare sector fell into the small-to-medium business category (1 to 100 employees), and outpatient care facilities like medical and dental offices comprised the bulk of these. Victims involved in publicly-disclosed incidents are spread more evenly in terms of organizational size, with a significant amount involving large hospitals and insurance companies.

Most organizations experiencing breaches fell into the small-to-medium business category; outpatient care facilities like medical and dental offices comprised the bulk of these.

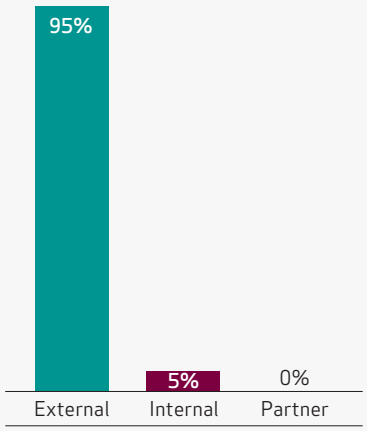
In addition to size, victim location is usually of interest in any discussion of data breaches. However, we find nothing extraordinary to note here except that most Healthcare victims in our data set were located in the United States. Undoubtedly, this is the result of caseload bias and U.S. disclosure laws more than it is a measure of relative risk across geographic boundaries.

THREAT AGENTS

Entities that cause or contribute to an incident are referred to as threat agents. VERIS recognizes three main categories of agents: those originating outside the victim organization (external), those inside the victim organization (internal), and those involving any third party sharing a business relationship with the victim (partner).

For those Healthcare organizations included within the DBIR data set, attacks were almost entirely the work of financially-motivated organized criminal groups acting deliberately and maliciously to steal information. These groups are notorious for knocking over smaller, low-risk targets in droves to nab personal and payment data for various and sundry fraud schemes. Insider jobs proved much less frequent, but they can't be ignored. When employees do go rogue, their ready access to and knowledge of information assets means they can do quite a bit of damage without expending a lot of effort.

Figure 1. Threat agents by percent of breaches in the Healthcare industry (DBIR data only)



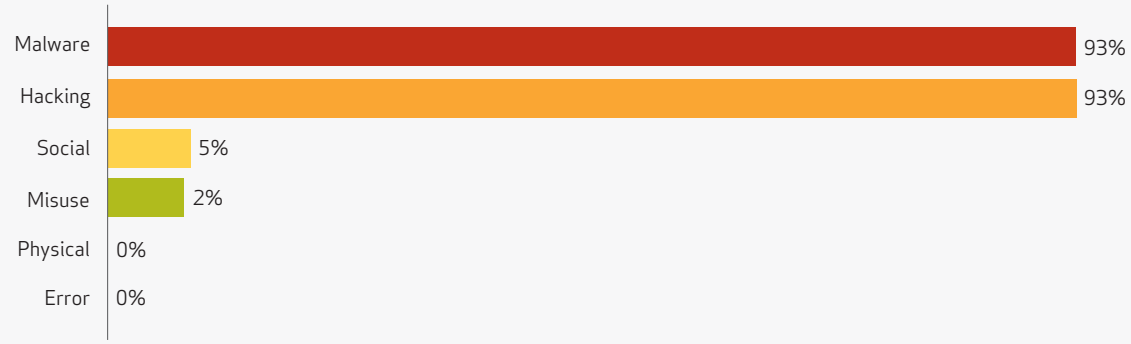
Among public disclosures in the Healthcare sector, the external/internal split is much more balanced. This, however, is largely due to lost laptops and other devices, which expose data and therefore must be reported (these are classified as internal error in VERIS). Examining public breaches with characteristics more in line with what typically winds up in the DBIR (i.e., incidents that require external forensics or law enforcement investigation) yields threat agent ratios that more closely resemble those found in Figure 1.

When employees go rogue, ready access to and knowledge of information assets means they can do quite a bit of damage without a lot of effort.

THREAT ACTIONS

Threat actions describe what the threat agents did to cause or to contribute to the breach. Within this industry, as illustrated in Figure 2, hacking and malware were both involved in nearly all breaches. This finding illustrates the fact that these two threat categories go hand-in-glove for most successful attacks on Healthcare organizations within the DBIR sample. These scenarios typically play out by the attacker scanning large swaths of the Internet for potential victims, hacking into the exposed systems (often via weak or stolen credentials), and installing some type of malware to capture data and/or fulfill other nefarious purposes. Table 1, which provides a more specific list of threat actions, gives more context around these and other attacks common within the Hacking and Malware categories.

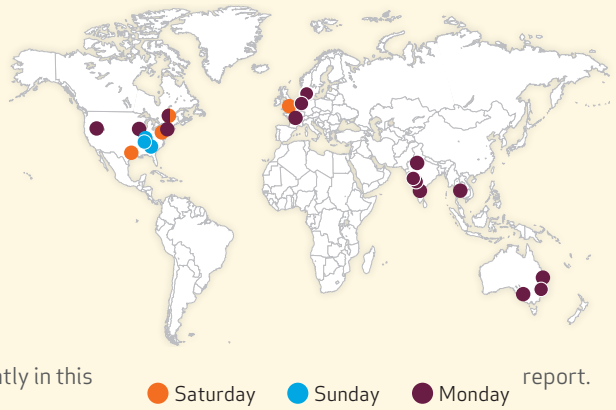
Figure 2. Threat action categories by percent of breaches in the Healthcare industry



This type of indiscriminate, quick, and often completely automated attack is the favorite of the aforementioned organized cybercriminal groups. The true story below, which included quite a few outpatient clinics and offices, illustrates just how easy and successful these types of attacks can be.

A THREE-DAY WORK WEEK

During our data collection for this report, we received a list from one of our law enforcement partners containing the dates and locations of a large number of incidents tied to a small organized criminal group operating out of Eastern Europe. It provided us the opportunity to study their behaviors and activities over about a six-month period. We found it fascinating and include it here in the hopes that it helps drive home notions like "industrialized," "rapid," "large-scale," and "opportunistic," which we reference frequently in this report.



Analysis of the data showed the attackers not only had no routine workweek, but they only worked an average of three days a week. During one particular three-day work week, they punched the clock on Saturday, Sunday, and Monday. They compromised 22 organizations across nine countries; Monday was the most productive, with 15 confirmed breaches registered that day (in purple). We would joke about "nice work if you can get it" but the jail time these guys are facing doesn't make for very nice work at all.

In the majority of cases (roughly three out of four), the attacker gained initial access by exploiting default or guessable credentials, usually via Internet-facing remote access services. Brute-force attacks (i.e., repeatedly attempting a "dictionary" of possible usernames/passwords) also made the top five. Once inside, savvy criminals begin scoping out the network and dropping malware. Backdoors appear especially popular in Healthcare breaches, where they more than double the average percentage across all industries.

In the majority of cases, the attacker gained initial access by exploiting default or guessable credentials, usually via Internet-facing remote access services.

Table 1. Threat action varieties by percent of breaches in the Healthcare industry

Rank	Variety	Category	Breaches
1	Exploitation of default or guessable credentials	Hacking	72%
2	Backdoor (allows remote access/control)	Malware	49%
3	Exploitation of backdoor or command and control channel	Hacking	49%
4	Unknown	Malware Hacking	43% 2%
5	Brute force and dictionary attacks	Hacking	20%
6	Disable or interfere with security controls	Malware	12%
7	Keylogger/Form-grabber/Spyware (capture data from user activity)	Malware	12%
8	Send data to external site/entity	Malware	12%
9	Use of stolen login credentials	Hacking	12%
10	Abuse of system access/privileges	Misuse	5%
11	Initiate brute force or dictionary attacks	Malware	2%
12	Theft	Physical	2%

Outside the DBIR data set, things look quite different—at least on the surface. Theft (Physical), loss (Error), and improper disposal (Error), which are negligible or nonexistent in Table 1, rise to the top of the ranks among threat actions contributing to publicly reported data breaches. Since it's difficult to conduct forensics on a device that isn't there, investigators aren't typically called in on cases like these. Furthermore, most of them are potential exposures (data-at-risk events) rather than confirmed data compromise, and thus do not meet the criteria for inclusion in the DBIR. Disclosed healthcare incidents that do cross this threshold start to look much like the DBIR findings, with various forms of Hacking rising to prominence.

COMPROMISED ASSETS

To get a sense for what threat agents are targeting, and thus what's most in need of protecting, it's important to analyze the types of information assets affected by data breaches. As a quick look at the chart will illustrate, POS systems and desktops were at the forefront of breaches in the Healthcare sector. At first glance, this may seem counterintuitive, since electronic health records would almost certainly be stored in a file or database server, and surely this is what the criminals are after. But this likely represents an incorrect assumption; most cybercriminals are more interested in accessing your bank account and applying for loans in your name than they are the details of your last medical exam.

Figure 3. Compromised assets by percent of breaches in the Healthcare industry*

Type	Category	
POS terminal	User Devices	64%
POS server (store controller)	Servers	48%
Desktop/Workstation	User Devices	38%
Database server	Servers	5%
Backup tapes	Offline Data	2%
Documents	Offline Data	2%
Unspecified/Other Server	Servers	2%

*Assets involved in less than 1% of breaches are not shown

For those in the Healthcare vertical, it may seem strange that POS systems would play such a prominent role—especially since medical professionals are trained to protect the confidentiality of patient information. While health records are extremely sensitive, they are not the only data handled within this industry worth protecting. Criminals—especially professional ones—are extremely adept at following the money trail. And, much like the Retail and Accommodation and Food Services industries, that trail often leads to the POS systems that process the co-pay for your check-up.

Although new standards have been developed in the last few years to restrict the storing of credit card data on POS devices, the data still must pass through them. If the attackers exploit weak credentials and place a backdoor or keylogger on that system, then all restrictions against unencrypted storage of payment card information are rendered moot. As mentioned previously, the high number of targets mixed with low or nonexistent defenses creates a concoction irresistible to criminals seeking to quench their thirst for easy money. Many smaller healthcare clinics and offices lack the expertise or resources to manage their own POS infrastructure, and therefore rely on third-party vendors to do it for them. This requires that some sort of remote access and administrative service be enabled on these systems. The victim assumes that vendors know their trade and implement appropriate security measures, but experience shows this trust is often misplaced.

While health records are extremely sensitive, they are not the only data worth protecting.

Of course, compromising POS systems are not the only way attackers force their way into healthcare clinics and offices. Desktops are commonly tied to breaches as well. It's not uncommon for an employee to click on a malicious e-mail attachment or visit a questionable site on a company desktop, consequently infecting the system with malware enabling an attacker to gain access to other devices within the network. Also, the more traditional forms of long-term storage like databases, backup tapes, and documents do appear in Figure 3, and should not be neglected.

Public disclosures in the Healthcare industry reinforce this last point. Tied to the much-increased frequency of thefts, losses, and disposal errors, user devices and storage media factor heavily among this broader data set. One of the more common scenarios is when a medical or dental office is burglarized and the computers taken. Most thefts like this target the hardware (for a quick flip) and not necessarily the data. Another recurring scenario illustrates the problem of paper records and their management—document disposal and theft were two major causes of exposures of offline data.

TIMELINE OF EVENTS

Response time is a good indicator of the maturity of an organization's security program. No one wants to be the victim of a breach, but if that unfortunate event arises, it's certainly better to know sooner rather than later, to limit exposure and take proper corrective measures. Among the major phases we consider in an event scenario are:

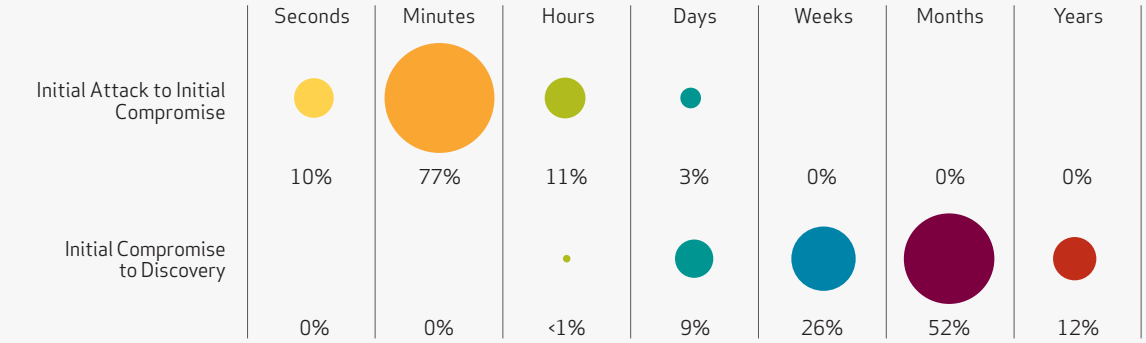
- **Initial Attack to Initial Compromise.** The time spanning from the first malicious action taken against the victim until an information asset is negatively affected.
- **Initial Compromise to Discovery.** The time spanning from when the first asset is negatively affected until the victim learns of the incident.

For a more complete accounting of incident scenario phases, please refer to the DBIR.

Unfortunately, the initial compromise occurs quite rapidly in most Healthcare incidents within our sample set. In over 85% of cases, mere minutes—or less—elapse before the victim's systems are infiltrated, and the exfiltration of sensitive data typically occurs quickly after that. These findings are largely related to the mode of attack and the uniformity of the target; it just doesn't take long to pop weak passwords on exposed POS devices that, for the most part, all process and store the same kind of data in similar ways.

In over 85% of cases, mere minutes—or less—elapse before the victim's systems are infiltrated.

Figure 4. Timespan of events by percent of breaches in the Healthcare industry



With the large number of automated and opportunistic attacks afflicting Healthcare organizations, it's hardly surprising that the perpetrators have often been and gone before anyone knows there's a problem. Close to two-thirds of all breaches go on for months before the victim learns that they've been compromised. What's more, they almost never detect it themselves; they're typically notified of their predicament by law enforcement or by payment card brands that have detected the incident through fraud analysis.

Close to two-thirds of all breaches go on for months before the victim learns that they've been compromised.

To add insult to injury, it often takes weeks or more before the breach is successfully contained. Once organizations realize they've been victimized, it's crucial they mount a swift and competent response. For many resource-challenged small-to-medium businesses, this means enlisting the support of external parties and/or law enforcement to stop the bleeding and get things on the mend.

We have no material observations to add with regard to the timeline of events for incidents outside our DBIR data, because such information is usually not included within public disclosures. From what we can glean from the data available, a drastically different story does not emerge.

RECOMMENDATIONS FOR HEALTHCARE

Because our dataset and, therefore our findings, evolve over time and encompass victims of different types, sizes, and geographic locations, creating a single list of recommendations that work equally and effectively for all organizations is unrealistic. Our basic advice—beyond covering the security essentials—is to adopt a common sense, evidence-based approach to managing security. Learn what threats and failures most often affect organizations like yours, and then make sure your security posture puts you in a position to thwart them.

Learn what threats and failures most often affect organizations like yours, and then make sure your security posture puts you in a position to thwart them.

Given the rather uniform nature of breaches within our data set affecting the Healthcare industry, however, it is relatively simple to sift through the evidence and create a short list of recommendations. In fact, the old adage that "an ounce of prevention is worth a pound of cure" is more than apt. For outpatient clinics and medical offices, it may seem unlikely that cybercriminals from across the world seeking fraud-ready data would find their way into your systems. But the fact remains that most attacks are directed against smaller companies, and those specializing in healthcare are no exception. The good news is that most can be prevented with some small and relatively easy steps. The following few tips are based on our research into scores of security breaches affecting companies in this industry.

The good news is that most attacks can be prevented with some small and relatively easy steps.

- **Change administrative passwords on all POS systems.** Hackers constantly scan the Internet for easily guessable passwords.
- **Implement a firewall or access control list on remote access/administration services.** If hackers can't reach your system, they can't easily steal from it.
- **Avoid using POS systems to browse the web.** Or anything else on the Internet for that matter.
- **Make sure your POS is a PCI DSS-compliant application.** Ask your POS vendor for additional information on this topic.

If a third-party vendor looks after your POS systems, we recommend asking them to confirm that these things have been done. If possible, work this into the contract. Following these simple practices will help save a lot of wasted money, time, and other troubles for your business and your customers.

Without examining the broader set of publicly-reported Healthcare breaches in more detail (or first-hand), our ability to offer recommendations is limited. However, we don't feel we're overstepping the bounds of evidence to suggest that encrypting user devices and media that contain medical and personal records is sufficiently justified. Done right, this will help avoid tripping the mandatory disclosure trigger next time an employee decides to "donate" his or her laptop, thumb drive, or tablet to the airport taxi charity.

To learn more about the findings in this report and our healthcare-centric security solutions, contact your account manager or visit verizon.com/enterprise/healthcare.

DATA BREACH INVESTIGATIONS REPORT

A study conducted by the Verizon RISK Team with cooperation from the Australian Federal Police,
Dutch National High Tech Crime Unit, Irish Reporting & Information Security Service,
Police Central e-Crime Unit, and United States Secret Service.

verizon.com/enterprise

© 2012 Verizon. All Rights Reserved. The Verizon name and logo and all other names, logos, and slogans identifying Verizon's products and services are trademarks and service marks or registered trademarks and service marks of Verizon Trademark Services LLC or its affiliates in the United States and/or other countries. All other trademarks and service marks are the property of their respective owners. MC15435 10/12.