verizon

Read time: < 4 minutes

2016 Data Breach Investigations Report

Healthcare

Almost three quarters of security incidents in healthcare in 2015 involved physical theft and loss, insider and privilege misuse and miscellaneous errors. While breach data was typically compromised in minutes or less, discovery often took months or more.

The Verizon 2016 Data Breach Investigations Report (DBIR) shows that the majority of data security incidents can be classified into one of nine patterns. Just three of these categories account for 73% of all healthcare data security incidents.

Physical theft and loss made up the largest share of all incidents in healthcare, at 32% of the total. This is a bigger problem for healthcare than for any other sector we analyzed this year. We'll look at these threats in greater depth and at how you can improve your defenses against them.

The Data Breach Investigations Report is the most comprehensive report of its kind. For the ninth time, it pulls together incident data from around the world, to reveal what's really happening in cybersecurity. The 2016 DBIR provides insights based on over 100,000 incidents from 82 countries, including 2,260 analyzed data breaches.

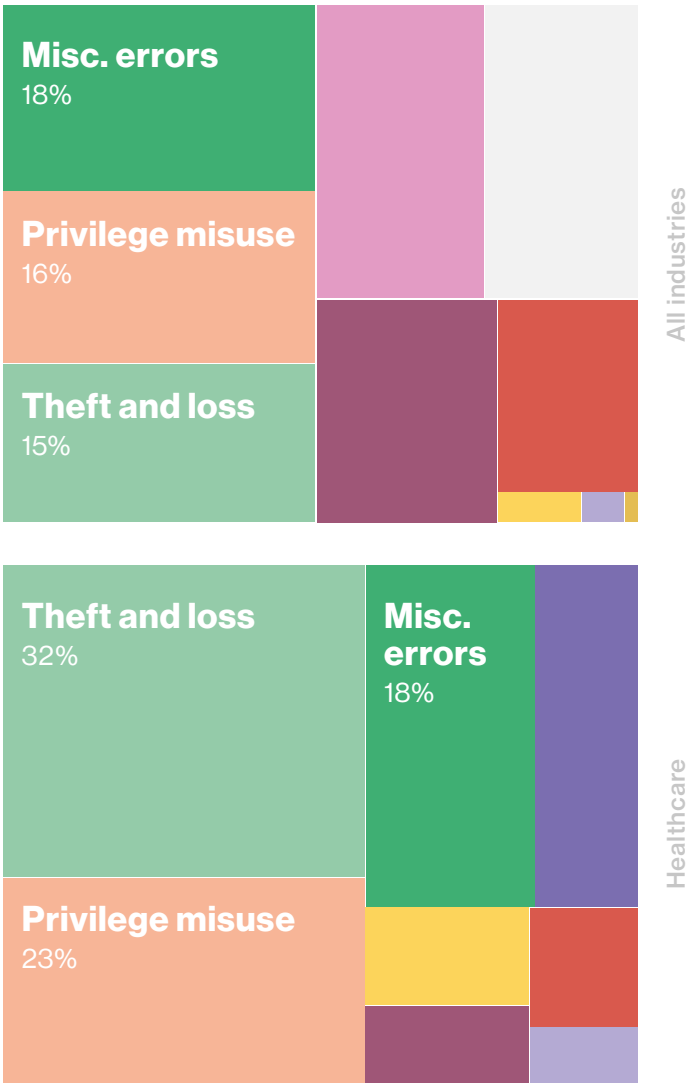

Figure 1: Incidents by pattern: All industries versus healthcare

Highlights of the 2016 DBIR

Prioritizing your defenses means understanding the threats you face. The 2016 DBIR enables you to do just that by providing insights based on over 100,000 incidents, including 2,260 analyzed data breaches.

The story is of cybercriminals motivated by money exploiting unforced errors:

- 89% of breaches had a financial or espionage motive.
- 63% of confirmed breaches involved leveraging weak, default or stolen passwords.
- 30% of phishing messages were opened in 2015; and 12% of targets clicked on the malicious attachment or link.
- 85% of successful exploit traffic was from the top 10 vulnerabilities. The other 15% covered 900 vulnerabilities.

This year's DBIR again focuses on the nine incident patterns we first identified in 2014, which cover over 85% of incidents. Understanding them will help you disrupt the dynamics of cybercrime and decrease the attackers' ROI.

Managing risks involved in collecting and storing protected health information (PHI) is critical to protect your bottom line and customer trust. The team behind the DBIR put PHI security under the microscope to help you identify threats and mitigate risks to your medical records. Read the Verizon 2015 Protected Health Information Data Breach Report.

Download the report >

Physical theft and loss

The physical theft and loss of assets is a big issue in healthcare, accounting for almost a third of all security incidents.

Physical theft of assets is a constant problem every year, across every industry. But the share of incidents it comprises in healthcare is larger than in any other industry in our dataset.

Stolen and lost information assets include laptops, desktops, mobiles, USB flash drives and paper documents. Looking across all sectors, theft of assets most commonly occurs in the victim's own work area (39%) or from the personal vehicle of the employee (34%). Despite this, the biggest risk in this category is from employees losing assets – that's 100 times more likely than theft.

What can you do?

- **Encrypt your data:** If stolen devices are encrypted it's much harder for attackers to access the data.
- **Train your staff:** Developing security awareness in your organization is critical. Include education on physical security as part of your orientation and ongoing training of employees.
- **Reduce use of paper:** Cut down on printing. Establish data classification rules and create a company policy covering the printing and transportation of sensitive data.

Insider and privilege misuse

Insider and privilege misuse accounts for 23% of security incidents reported in healthcare in the 2016 DBIR – it accounts for 16% of security incidents across all sectors. And it's the leading cause of confirmed data breaches, where data was stolen, in healthcare.

Insider and privilege misuse is often carried out by disgruntled employees or ex-employees using their access rights to take confidential information for personal financial gain. But there are also cases of collusion of insiders with external third parties – and where business partners, such as vendors, misuse their privileged access.

What can you do?

- **Monitor user behavior:** Put processes in place to track daily system usage – particularly by anyone with access to data they could profit from, such as protected health information, personally identifiable information or financial account details.
- **Track USB usage:** Don't leave yourself in a position where you only find out that an employee has taken data after they've left.
- **Know your data:** To protect your data, you need to know what data you have, where it is, and who can access it. Where possible, restrict data access to those who really need it. Make sure to update your user accounts as soon as employees leave your organization or change job role.

Miscellaneous errors

The next on the list of incident patterns is miscellaneous errors, accounting for 18% of the total.

Many incidents were caused by employees sending emails or documents to the wrong recipient. There were also cases where information was published to an unintended audience (e.g. public disclosure).

Any loss of patient data or other sensitive information could have a negative impact on a healthcare organization's relationship with its patients, partners and the public.

Human error can never be completely eliminated, but in the majority of cases the likelihood of an error occurring can be significantly reduced using the right processes and controls.

What can you do?

- **Learn from your mistakes:** Talk about errors. Keep a record of common mistakes and use them in training materials for security awareness.
- **Map mistakes:** Map the most common mistakes. With this data, establish effective controls to help minimize the frequency with which errors occur and mitigate the damage when they do take place.
- **Dispose securely:** When assets are ready for disposal, make sure that there is a documented procedure for wiping them before they are trashed or resold.

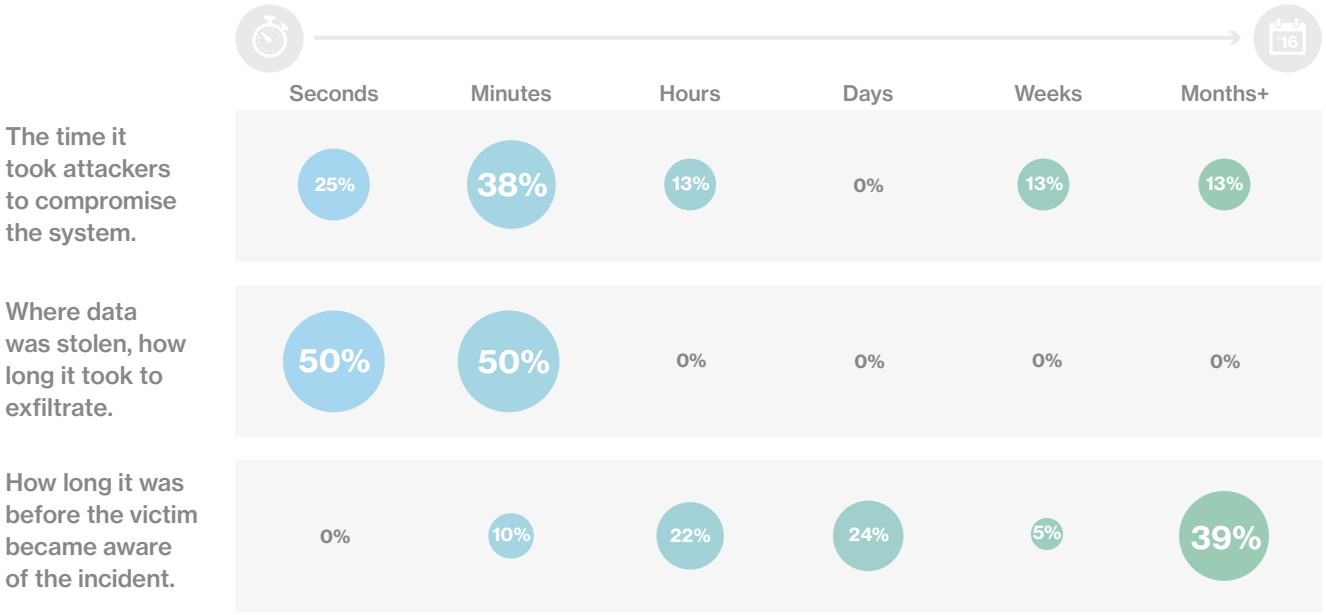

Figure 2: Incident timeline for healthcare

Time to discover an incident

The healthcare industry is slow to detect security incidents and breaches, where data is disclosed. Although 56% of incidents were discovered in days or less, 39% remained undiscovered for months or more. And healthcare systems were compromised in minutes or less in 63% of cases. This gives successful attackers plenty of time to search for sensitive – and potentially lucrative – patient records. What's worse, in cases of confirmed data breaches – where data was stolen – discovery took months or more in 56% of cases.

You have to know what you're really up against. Only then can you get the right data security solutions for your organization. Build your defences on the DBIR. Get the vital insights you need today.

Read the report now ›

How can we help?

Our Managed Security Services (MSS) platform processed over 61 billion events in 2015. And we operate nine security operations centers on four continents. We were positioned as a leader in the 2015 Gartner Magic Quadrant for Managed Security Services, Worldwide.

We put our unique security insight to work every day in the solutions we provide – to help you guard against the threats you face.

Our Data Protection service provides guidance for a data protection governance framework and its implementation, helping you deliver a mature Data Loss Prevention (DLP) program, including rule and report documentation.

Our Application Vulnerability Assessment service tests platform and application security using a mix of consultant expertise and automated tools, including penetration testing where appropriate.

Our Rapid Response Retainer program can help you plan and defend against possible threats, and take fast action to identify and contain incidents when they take place. This helps you proactively secure your customers' and partners' sensitive data and maintain their business and trust.

VerizonEnterprise.com