

The logo for NetDiligence, featuring the word "NetDiligence" in a blue serif font with a registered trademark symbol. The letter "i" in "Diligence" has a small orange dot above it.

NetDiligence®

The title "2017 CYBER CLAIMS STUDY" is written in white, uppercase, sans-serif font on a large orange triangular background that points towards the right.

2017  
CYBER  
CLAIMS  
STUDY

The text "2018 Spotlight HEALTHCARE" is displayed in a grey, sans-serif font. "2018 Spotlight" is on the top line and "HEALTHCARE" is on the bottom line, both centered horizontally.

2018 Spotlight  
HEALTHCARE

The logo for AllClear ID, consisting of the text "AllClear ID" in white, sans-serif font inside a blue, rounded rectangular shape with a white border.

AllClear ID

The logo for RSM, featuring a horizontal bar with a green segment on the left and a blue segment on the right, positioned above the letters "RSM" in a bold, black, sans-serif font.

RSM



## Introduction

As an adjunct to our annual *Cyber Claims Study*, NetDiligence® is proud to release the first in a series of “deeper dive” reports.

The annual NetDiligence® *Cyber Claims Study* uses actual cyber liability insurance reported claims to illuminate the real costs of incidents from an insurer’s perspective.

Our objective for these studies is to help risk management professionals and our cyber insurance partners understand the true impact of data insecurity by consolidating cybersecurity breach claims data from multiple insurers so that the combined pool of claims is large and diverse enough that it allows us to ascertain a reasonable snapshot of the costs and project future trends.

## Summary

Healthcare is under attack. Hackers, malware and viruses, rogue employees, ransomware, lost and stolen devices, staff mistakes, system glitches, and the failure to properly handle paper records have all contributed to large losses in the healthcare sector.

Of the 591 claims in the 2017 study, 103 pertained to healthcare. From the examination of those 103 claims, we offer the following key findings.



## Breach Costs and Records Lost

While healthcare claims comprised **17% of claims** in the 2017 dataset, they represented **28% of total breach costs** (\$65M of \$229M).

The **average** number of records exposed in a healthcare breach was **1.6M**. However, the **median** number of records exposed was a modest **1K**.

Breaches that exposed Protected Health Information (**PHI**) were **substantially smaller** than breaches that exposed Personally Identifiable Information (**PII**) – 386K vs. 5.2M records on average. The **total average breach cost** for PHI was also correspondingly lower – **\$475K vs \$1.85M** for PII.

The **median per-record cost** in healthcare was **lower** than all other sectors (\$28 vs \$47). However, due to several very large settlements involving very few records, the average per-record cost for healthcare was very high.

# Cost of Post Breach Services



\*This may be partially due to the very large numbers of records exposed/people affected (>97M). Another factor may be that healthcare breaches often expose both PHI and PII.  
\*\*This despite anecdotal evidence that State Attorneys General (AGs) and the Department of Health and Human Services Office of Civil Rights (HHS OCR) are actively levying fines on healthcare entities.

## Causes of Loss

Approximately **63%** of healthcare breaches were caused by **criminal or malicious activity**.

**Ransomware** continued to be a frequent and costly event, representing **10% of all healthcare claims** in our dataset. The **average cost** for a ransomware incident was **\$76K**.

**Hacking** was the **most common cause** of loss in healthcare (20%), with an average breach cost of **\$2.4M**.



## Discussion

### Events and Incidents

Incidents in which a hacker used malicious code required the use of all crisis services to respond. Criminal acts exposed 80M PII and 17M PHI records, and were the reason that the healthcare sector had the highest total notification (\$37.1M) and credit/ID monitoring (\$6.6M) costs.

### Are Third-Parties Your Weakest Link?

Third-parties (vendors) were the second biggest cause of loss, exposing nearly 4M records and incurring the highest legal damages. Information leaks revealing potential intrusions and data breaches can have legal consequences. The organization may be required to report the problem to comply with financial and privacy regulations.

### Social Engineering: Up Close and Remote

Social engineering, whether through physical encounters (phone, face-to-face) or remote digital methods (email) have costly ramifications. Our dataset was split evenly between physical and digital social engineering methods. Social engineering that led to unauthorized access to patient records and employee W-2s resulted in healthcare having the highest per-record cost of all business sectors.

### Rogue Employees: Past and Present

Employees who access, view or steal sensitive, protected or confidential patient information fall into two categories: current employees and terminated employees whose user credentials were not revoked. Events caused by rogue employees may involve forensics, notification, and credit/ID monitoring costs. Our data shows that in rogue employee incidents the costs for legal guidance, legal damages defense and/or legal regulatory defense are high.

### Protecting Assets

Laptop theft is still happening! Unsecured laptops with unencrypted hard drives typically result in notification, credit/ID monitoring, and legal defense costs. In our study, the average cost of a stolen device was \$37K.

## Ransomware

By targeting the user environment through remote communication mediums, criminals exploit the end user to breach the security of the corporate environment. Business recovery and lost income account for 90% of the cost of these claims.

## Staff Mistakes

Unlike brute force attacks, which use specific tools to relentlessly pursue their objectives, staff mistakes are one-time events, caused by human error. These incidents arise out of accidental email exchanges and improper paper disposal of PHI records. The number of claims caused by employee mistakes is comparable to the number of claims caused by rogue insiders and just-terminated employees. However, on a per-record basis, the cost of inadvertent mistakes is 98% higher than the cost of criminal activity.

## A Note on Methodology

Our data collection, analysis, and reporting methodology are described in detail in the full 2017 NetDiligence® *Cyber Claims Study*.

## Contact Us

For more information about NetDiligence® or any of our service offerings, please visit us at [NetDiligence.com](https://www.netdiligence.com), email us at [management@netdiligence.com](mailto:management@netdiligence.com), or call us at 610.525.6383.

