NetDiligence®

2017 CYBER CLAIMS STUDY

2018 Spotlight

HEALTHCARE

AllClear ID

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, email us at management@netdiligence.com, or call us at 610.525.6383.

Appendices

Please note that, due to the re-examination and reclassification of certain claims, the overall numbers reported here may not match the numbers published in the 2017 *Cyber Claims Study*.

Table 1

Healthcare - Overall	Cases	Median	Average	Total
Records	69	1,000	1,618,817	111,698,377
Payouts	91	32,264	498,781	45,389,045
Breach Costs	99	55,000	654,080	64,753,919
Per-Record Cost	66	28.42	27,021	
Crisis Management				
Forensics	42	37,545	166,432	6,990,154
Notification	37	15,000	1,025,210	37,932,772
Credit/ID Monitoring	31	23,610	246,169	7,631,244
Legal Guidance	69	14,168	57,279	3,952,236
Other Crisis	13	9,500	123,155	1,601,018
Total Crisis	86	40,955	675,668	58,107,424
Other				
Legal Damages - Defense	18	19,706	115,667	2,082,001
Legal Damages - Settlement	3	50,000	115,582	346,747
Regulatory Action - Defense	5	100,000	133,077	665,386
Regulatory Action - Fines	0			
PCI Fines	0			
Business Income Lost	1	33,000	33,000	33,000
Recovery Expense	3	30,000	157,433	472,299

Table 2

Healthcare - Cause of Loss Criminal Actions	Cases	Median	Average	Total
Records	41	3,942	2,722,686	111,630,124
Payouts	58	49,213	750,241	43,513,972
Breach Costs	63	63,212	971,532	61,206,520
Per-Record Cost	40	11.99	1,904	
Crisis Management				
Forensics	34	42,682	200,084	6,802,857
Notification	24	26,118	1,573,662	37,767,894
Credit/ID Monitoring	21	30,002	344,592	7,236,440
Legal Guidance	43	19,478	75,580	3,249,953
Other Crisis	10	11,500	158,440	1,584,402
Total Crisis	55	56,938	1,029,846	56,641,547
Other				
Legal Damages - Defense	12	32,206	117,207	1,406,480
Legal Damages - Settlement	1	264,247	264,247	264,247
Regulatory Action - Defense	5	100,000	133,077	665,386
Regulatory Action - Fines	0			
PCI Fines	0			
Business Income Lost	1	33,000	33,000	33,000
Recovery Expense	3	30,000	157,433	472,299

Criminal Actions include the activities of hacker, malware, rogue employees, and thieves (hardware, social engineers).

Table 3

Healthcare - Cause of Loss Non-Criminal Actions	Cases	Median	Average	Total
Records	27	230	2,491	67,253
Payouts	34	22,500	55,427	1,884,511
Breach Costs	36	44,727	98,817	3,557,399
Per-Record Cost	26	187	65,663	
Crisis Management				
Forensics	8	9,598	23,412	187,297
Notification	13	4,000	12,683	164,878
Credit/ID Monitoring	10	8,391	39,480	394,804
Legal Guidance	26	14,168	27,011	702,283
Other Crisis	3	1,658	5,539	16,616
Total Crisis	31	31,000	47,286	1,465,877
Other				
Legal Damages - Defense	6	5,299	112,587	675,521
Legal Damages - Settlement	2	41,250	41,250	82,500
Regulatory Action - Defense	0			
Regulatory Action - Fines	0			
PCI Fines	0			
Business Income Lost	0			
Recovery Expense	0			

Non-criminal actions include lost devices, improper disposal of paper records, staff mistakes, and system glitches.