corax CLYDE&CO

2018

Cyber Breach Insights

Key Drivers Behind Cyber Insurance Claims

corax

The Corax mission is to help the insurance industry sell more cyber insurance.

Corax is a cyber risk analytics platform that puts a dollar value on cyber exposure for single insurance policies and portfolios as well as points of aggregation and disaster scenarios.

Corax is focused on the entire insurance value chain. From prospects to brokers and insurers, including their re-insurance counterparts, Corax makes generating leads, pricing exposure, assessing cyber hygiene, managing portfolios and modelling disaster scenarios straightforward and efficient.

We access unique data on claims as well as data on breach and business interruption events to inform our modelling.

Our differentiators are anchored in transparency of method, production of exceedance probability curves for organizations and portfolios, the provision of exposure management metrics in real-time and flexible commercial terms.

www.coraxcyber.com

Marcus Breese

Head of Insurance Innovation
and Strategy, Corax

marcusbreese@coraxcyber.com
+44 (0) 203 608 9063

CLYDE&CO

Clyde & Co is recognized as the world's leading international insurance and reinsurance law firm, and is one of the first and only law firms to specialize in cyber liability insurance.

Our cyber team has worked on over 3,000 data breaches across the world, ranging from small single person breaches to some of the largest and most complicated multi-jurisdictional breaches to date.

In addition, our team regularly assists insurers with the drafting of cyber policy wordings.

Clyde & Co has 3,300 staff in over 40 offices across six continents.

www.clydeco.com

Christina Terplan

Partner, Clyde & Co

christina.terplan@clydeco.us
+1 415 365 9821

CONTENTS

01

EXECUTIVE SUMMARY

Law firm Clyde & Co and risk analytics platform Corax have collaborated to bring you a joint white paper identifying the **key drivers of frequency and cost for cyber insurance claims**. This paper moves beyond major breaches to examine the day to day breaches that most businesses are experiencing.

Unlike other breach reports, this paper tracks each **invoiced cost** or loss amount associated with a covered breach event.

Anonymized data was sourced from **321 data breach events** where Clyde & Co acted as monitoring counsel for cyber insurer clients. The breach events were reported to insurers between **2014** and **2015.** Files were selected randomly.

321

Breach events

1. SMBs reported the highest number of breaches.

90%

of organizations that experienced breaches are small and medium sized.

Most frequently breached

Healthcare & Pharmaceuticals
Leisure, Retail & Hospitality

$18K

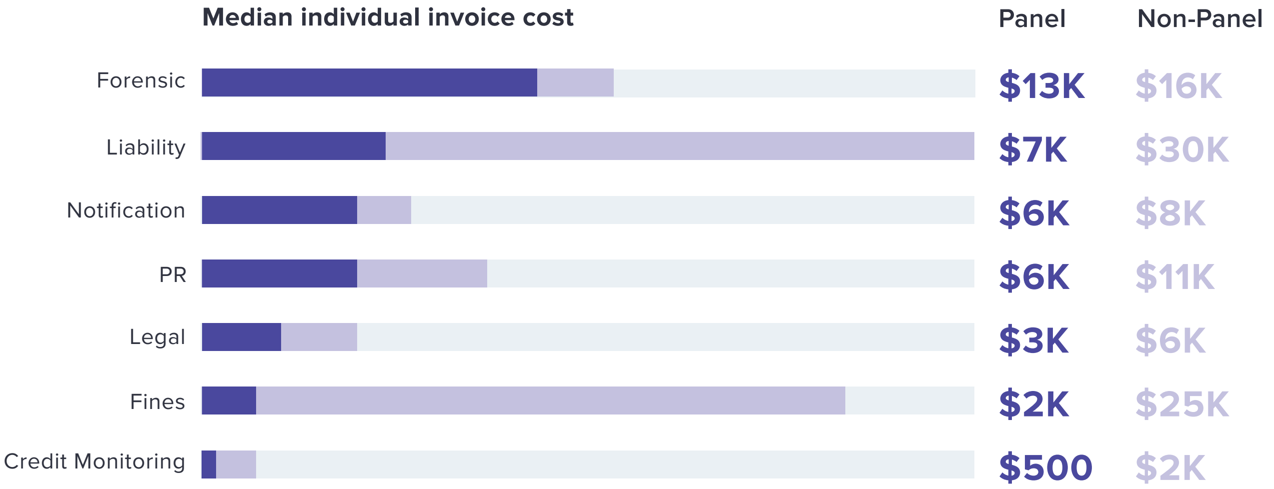
Median event cost

Most expensive breach

Leisure, Retail & Hospitality

2. Panel vendors make a difference.

Per record panel costs are 50% lower than non-panel.



Median individual invoice cost	Panel	Non-Panel
Forensic	$13K	$16K
Liability	$7K	$30K
Notification	$6K	$8K
PR	$6K	$11K
Legal	$3K	$6K
Fines	$2K	$25K
Credit Monitoring	$500	$2K

■ EXECUTIVE SUMMARY

3. There is no single solution to breach prevention.

Event types:

29%
Unauthorized Access or Manipulation (94)

24%
Ransomware (76)

18%
Unauthorized Disclosure (58)

11%
Malware (34)

10%
Phishing (33)

8%
Other (28)

Stolen Device 7% (22)
Lost Device 1% (4)
Improper Disposal 0.6% (2)

4. Record type impacts duration.

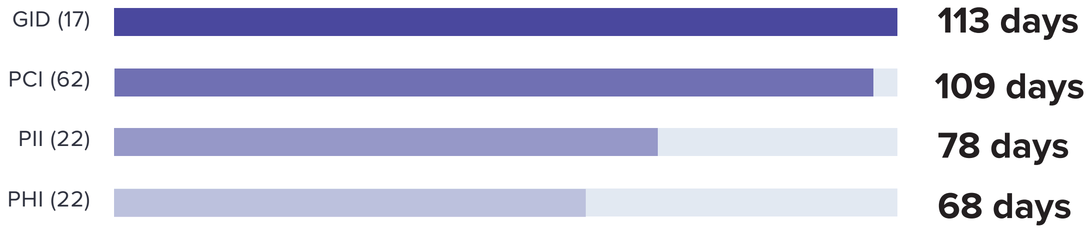
1.5x

Social security numbers and credit card records increase event duration by 1.5 times

78 days

Median event duration

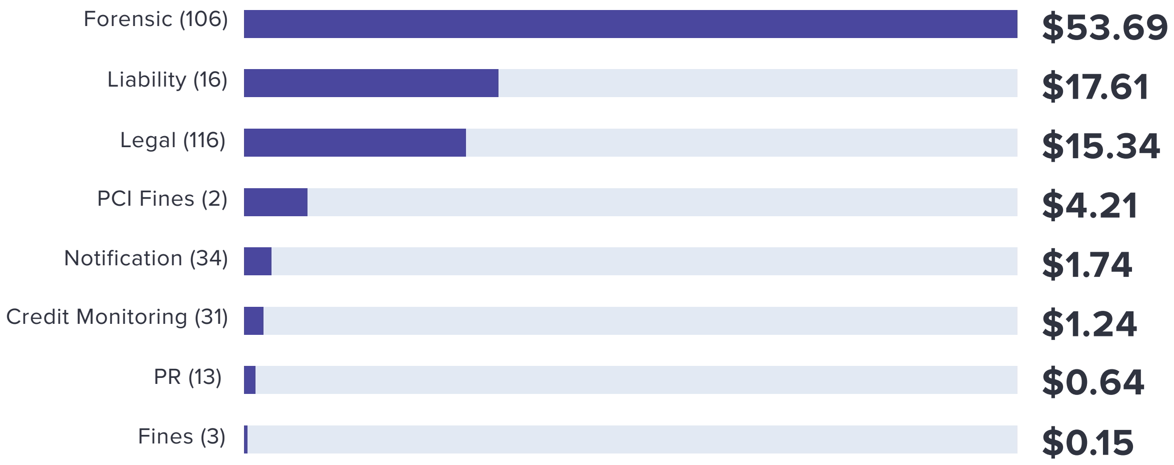
Median duration by record type:



■ EXECUTIVE SUMMARY

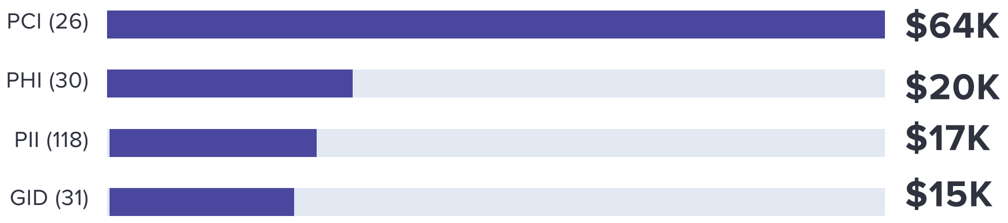
5. Forensics costs were one of the most common and most expensive types of costs, but were not driven by record count.

Median cost per record by type



6. Credit card data breaches were 3x more costly than other record types.

Median event cost



02
OVERVIEW OF THE DATA

SOURCE & QUALITY

For the purpose of this report, anonymized data was sourced from 321 data breach event closed claims files where Clyde & Co acted as monitoring counsel for cyber insurer clients (the data set).

The breach events were reported to insurers between 2014 and 2015. This date range allows reasonable time for third party liabilities to be resolved.

Files were selected randomly and the goal was to obtain data on “everyday” breach events rather than major breaches that are the subject of newspaper headlines.

To this end, the data does not include outlier events, which we defined as breaches involving more than 40M records.

The report does not include business interruption events, these will be the subject of a future analysis.

Unlike other breach reports, this analysis tracks the invoiced cost or loss amounts associated with a covered breach event. The invoices include data on:

- Vendors used*
- The nature of service(s) provided
- Date of invoices
- Loss amounts
- Breach cause
- Number of records impacted
- Insured industry

**Where at least one vendor formed part of the breach response*

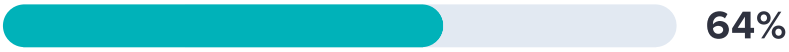
OVERVIEW: BASIC STATISTICS

*Throughout the report, data shown in **( )** within a table represents a **count.***

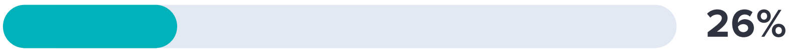
Organizations within the data set were categorized by and distributed within the following categories:

Size

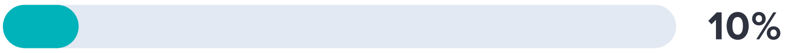
SMALL (205)
Organizations that purchased policies from program facilities aimed at small business e.g. solo practitioners and start-ups.



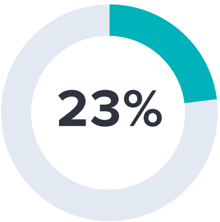
MEDIUM (84)
Organizations not purchasing policies from program facilities, with revenues **less than $1 billion.**



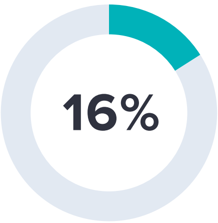
LARGE (31)
Organizations with annual revenues **greater than $1 billion.**



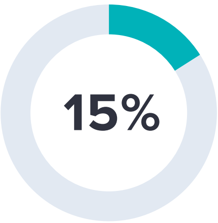
Industry



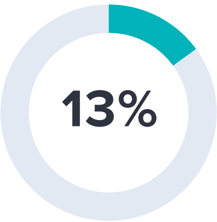
Healthcare/ Pharmaceuticals (75)



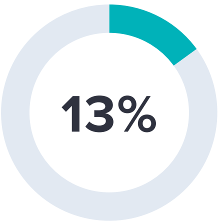
Leisure/Retail/ Hospitality (51)



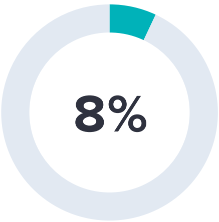
Financial Services (48)



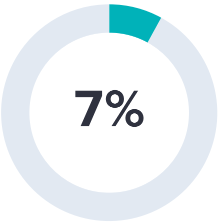
Professional Services (42)



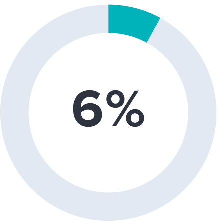
Industrial/Energy* (42)



Education (25)



Government (22)



Technology/Media/ Telecommunications (18)

* *Construction, Energy, Utilities, Manufacturing, Production, Non-Professional Services, Transport, Logistics*

OVERVIEW: BASIC STATISTICS

The distribution of industry sectors by size

	TOTAL	SMALL	MEDIUM	LARGE
Healthcare/Pharmaceuticals	23% (75)	47% (35)	37% (28)	16% (12)
Leisure/Retail/Hospitality	16% (51)	45% (23)	39% (20)	16% (8)
Financial Services	15% (48)	69% (33)	27% (13)	4% (2)
Professional Services	13% (42)	83% (35)	10% (4)	7% (3)
Industrial/Energy*	13% (42)	93% (39)	7% (3)	0% (0)
Education	8% (25)	60% (15)	32% (8)	8% (2)
Government**	7% (22)	64% (14)	18% (4)	14% (3)
Technology/Media/ Telecommunications	6% (18)	72% (13)	22% (4)	6% (1)

* *Construction, Energy, Utilities, Manufacturing, Production, Non-Professional Services, Transport, Logistics*

** *Organization size information was not available for one incident in this research data, hence percentages in this example do not total 100.*

Insights

Healthcare/Pharmaceuticals had the highest number of breach events, almost 50% more than **Leisure/ Retail/Hospitality**, the next highest industry.

Leisure/Retail/Hospitality, Financial Services, and **Professional Services** had very similar numbers of breach events.

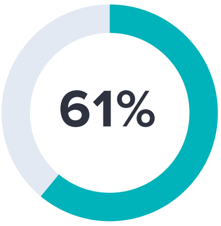
Small organizations consistently had the highest number of breaches.

OVERVIEW: BASIC STATISTICS

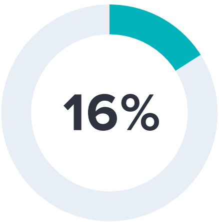
Record type

Note: There were some incidents that involved multiple record types, hence percentages in this example do not total 100.

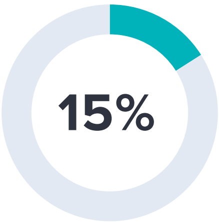
PII
Personally Identifiable Information
(195)



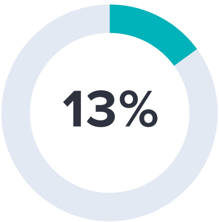
GID
Government ID
(50)

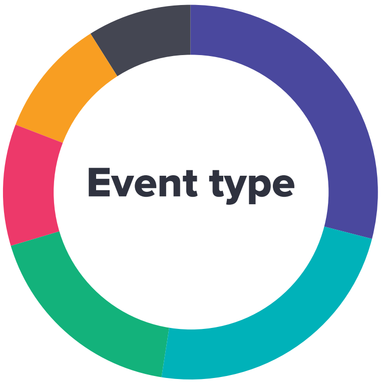


PHI
Protected Health Information
(47)



PCI
Payment Card Information
(43)





29% Unauthorized Access or Manipulation (94)

24% Ransomware (76)

18% Unauthorized Disclosure (58)

11% Malware (34)

10% Phishing (33)

8% Other (28)
7% Stolen Device (22)
1% Lost Device (4)
0.6% Improper Disposal (2)

Insights

There is no single solution for preventing data breach events. A combination of both technological and human training solutions is required.

Data breach events involving **unauthorized access** or **manipulation** (29%) were caused by internal and external parties. User rights management and the use of data at rest encryption is clearly an important factor in preventing data breach events.

The prevalence of **ransomware** (24%) as the second most common breach event type fits with our experience. Given the data set contains events from 2014 / 2015 and the Office of Civil Rights' 2016 guidance on ransomware events, our expectation is that these events will now be reported more frequently.

Just 8% (26) of events were due to **lost or stolen devices**. Our experience would suggest that historically these events would have been more prevalent within the data set.

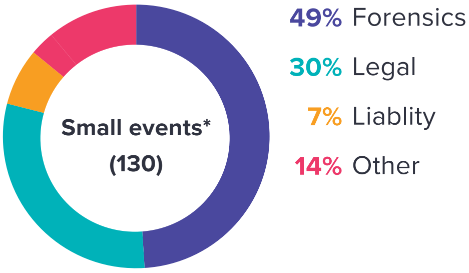
OVERVIEW: BASIC STATISTICS

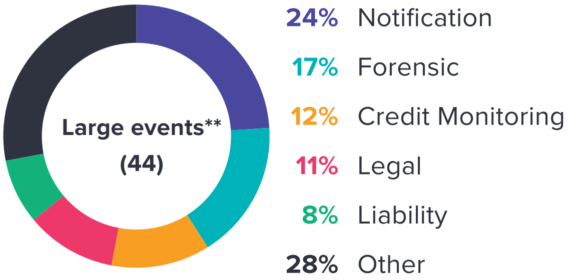
Breach events

Event cost (174 events with costs, 147 events with no costs)

$444K	$18K	$21M
MEAN	MEDIAN	MAXIMUM

Cost proportions (for **small** and **large** events)





**Small is defined as the lower 75% of events by total cost.*
***Large is defined as the upper quartile of events by total cost.*

Number of records (200 events with non-zero number of records)

276K	120	40M
MEAN	MEDIAN	MAXIMUM

Cost per record (105 events with invoices and non-zero number of records)

$2.9K	$30	$166K
MEAN	MEDIAN	MAXIMUM

Insights

121 of the breach events had a zero record count meaning **no records were impacted.**

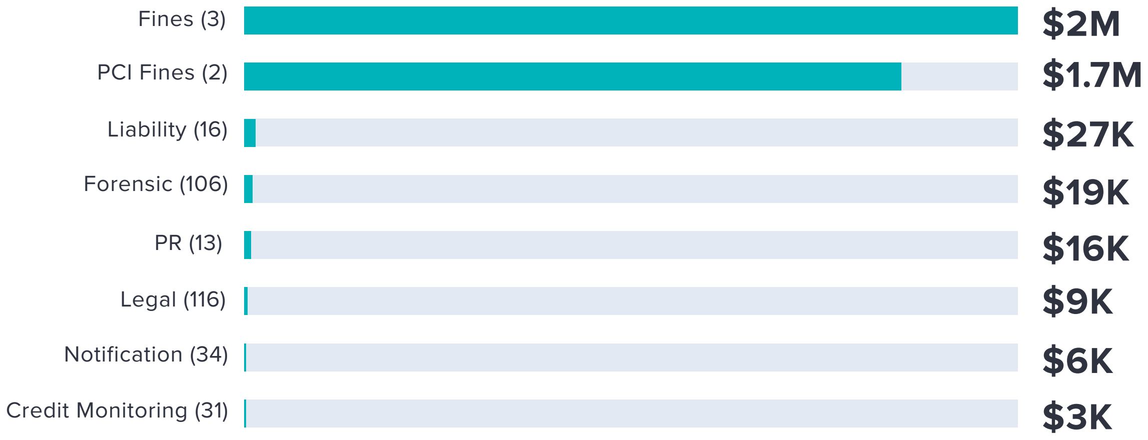
The distribution of breached records is skewed significantly by large incidents. **50%** of the non-zero record breaches had a count of 120 records or less. This fits with our experience. The vast majority of breach events have zero or low numbers or breached records.

These distributions mirror the distribution of losses within the Corax Risk Analytics platform.

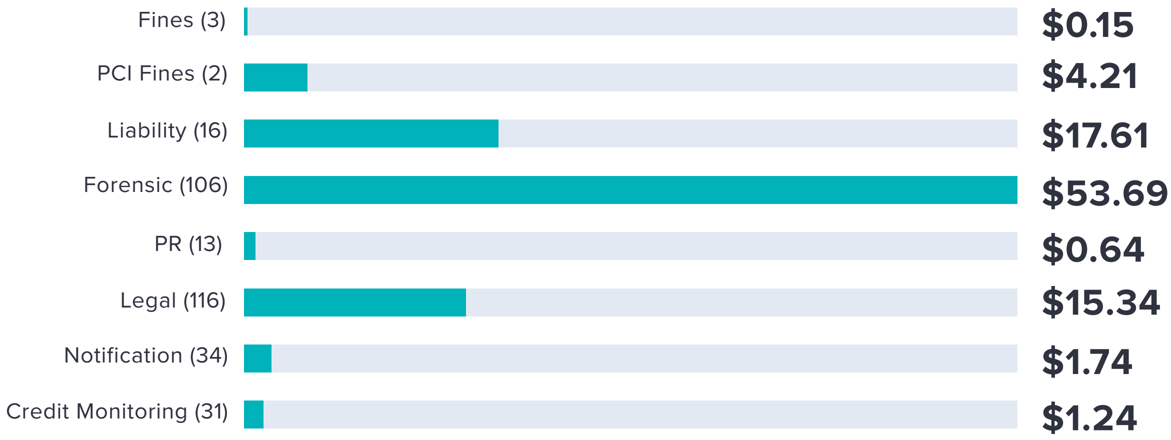
■ OVERVIEW: BASIC STATISTICS

Costs by type

Median cost by type



Median cost per record by type



Insights

The most common invoice types were **Legal** (116) and **Forensics** (106) and were significantly more prevalent than the next invoice type being **Notice** (34).

The count for **Fines** (3) and **PCI fines** (2) was low. This fits with our expectations given the majority of breach events do not result in fines.

The distribution of invoices by count contrasts with the distribution by cost.

When considering costs, **Fines** & **PCI Fines** ($2m and $1.7m) were by far the most expensive component of the total cost of a claim. The next highest being **Liability** ($27k) followed by **Forensic** ($19k).

In contrast, when examining cost type per record, **Fines** & **PCI Fines** were not cost drivers. The highest costs per record was **Forensic** ($53.69) which were 3.5 times the next largest cost type per record, **Liability** ($17.61). This significant difference could be explained by the fact that cost per record is an inappropriate measure when considering **Forensic** costs since they are driven largely by complexity of attack.

OVERVIEW: BASIC STATISTICS

Record types

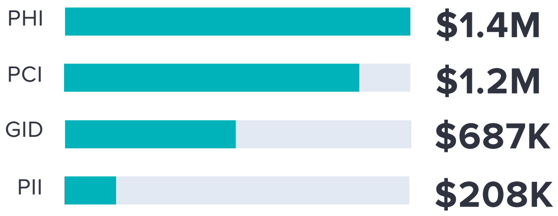
PII:
Personally Identifiable Information

GID:
Government ID

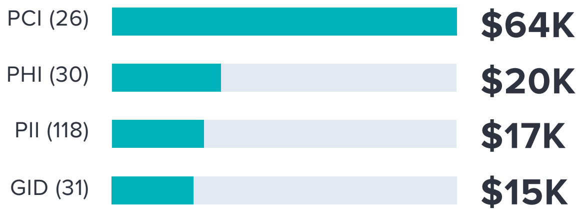
PHI:
Protected Health Information

PCI:
Payment Card Information

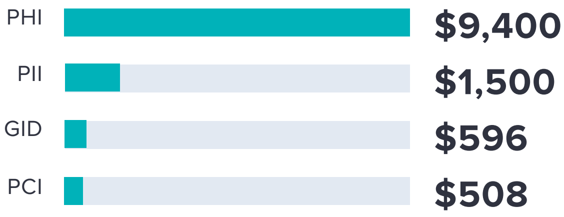
Mean event cost



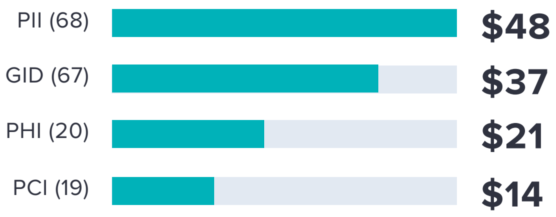
Median event cost



Mean event cost per record



Median event cost per record



Insights

Breach events involving credit card data ($64k) were **3x more costly** than those where card data was not impacted. The average cost of breach events involving non-PCI record types was $17k and these costs don't vary significantly by type.

In our experience, the high cost per record of credit card breaches is driven by the cost of:

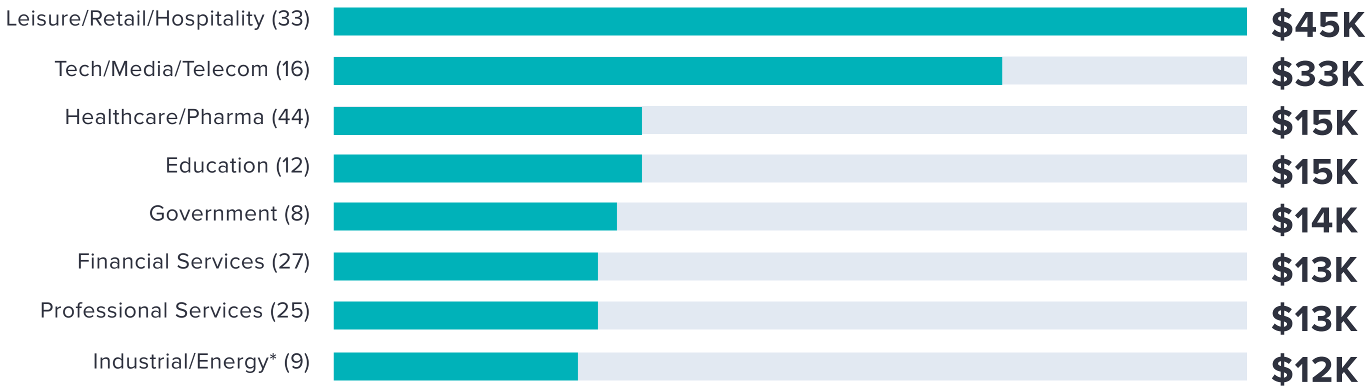
- **PCI fines** (at $1.7m, this was the second highest median cost type within the data set) and
- **Hiring two forensic companies** (one engaged by the card brands and a second by the insured.)

Additionally, if a PCI Forensic Investigator is required, insureds typically engage privacy counsel to mitigate **PCI fines.**

OVERVIEW: BASIC STATISTICS

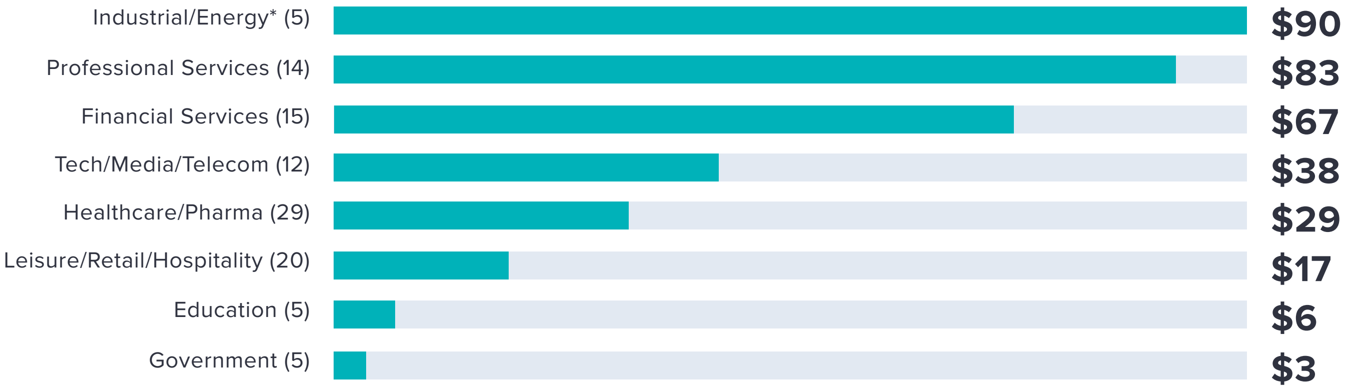
Industries

Median event cost



*Construction, Energy, Utilities, Manufacturing, Production, Non-Professional Services, Transport, Logistics

Median event cost per record



*Construction, Energy, Utilities, Manufacturing, Production, Non-Professional Services, Transport, Logistics

Insights

Breach events within **Leisure/Retail/Hospitality** were on average the most expensive ($45k) and the second most common industry sector (33). These breach events were 36% more expensive than the next most expensive industry sector **Technology/Media/Telecommunications** ($33k), which ranked 5th out of 8 in terms of frequency.

The most common breach events occurred in the **healthcare industry** (44) and these were similar in cost ($15k) to all other industry types with the exception of **Leisure/Retail/Hospitality** ($45k) and **Technology/Media/Telecommunications** ($33k).

The industry type distribution is at least partially explained by the types of records held by each industry.

OVERVIEW: BASIC STATISTICS

Cost vs non-cost events

174

COST EVENTS

147

NON-COST EVENTS

Industry breakdown:

	COST	NON-COST
Education	48% (12)	52% (13)
Financial Services	56% (27)	44% (21)
Government	37% (8)	63% (14)
Healthcare/Pharmaceuticals	59% (44)	41% (31)
Leisure/Retail/Hospitality	65% (33)	35% (18)
Professional Services	60% (25)	40% (17)
Industrial/Energy*	21% (9)	79% (33)
Technology/Media/ Telecommunications	89% (16)	11% (2)

**Construction, Energy, Utilities, Manufacturing, Production, Non-Professional Services, Transport, Logistics*

Insights

The split between **cost** versus **non-cost** events was relatively even with a slight bias (60/40) for those industries with the most events. The exceptions were:

1. **Industrial/Energy** due to comparatively low record counts and the biggest exposure being business interruption.

2. **Technology** companies because of high numbers of records that were impacted.

OVERVIEW: BASIC STATISTICS

Cost vs non-cost events
(with non-zero cost events removed)

Number of records (for the 112 events with cost)

485K	353	40M
MEAN	MEDIAN	MAXIMUM

Number of records (for the 88 events without cost)

10K	7	800K
MEAN	MEDIAN	MAXIMUM

Correlation between records and cost:

1 = High correlation
0 = No correlation

0.94	0.89	0.83
Notification	**Liability**	**Legal**
0.69	0.64	0.05
Forensic	**PR**	**Credit Monitoring**

Insights

From our experience, an insured that has a low breach count event is more likely to handle that event internally. For higher volume breaches insureds are more likely to seek outside assistance.

We assume that the no-cost event involving 800k records did not require notification.

There is a **strong positive correlation** between notification, legal costs and liability and breached record count. The positive correlation between breached records and **Forensic** and **PR** costs is less strong. This is in line with our experience. These costs typically have a fixed contract value associated with them.

Credit Monitoring costs are barely correlated to record count. This can be explained by the cost structure of credit monitoring and the low take up rate.

03

DURATION

Duration is defined as the elapsed time between dates of first and last invoice. The date of discovery predates the date of the first invoice, typically by approximately 30 days.

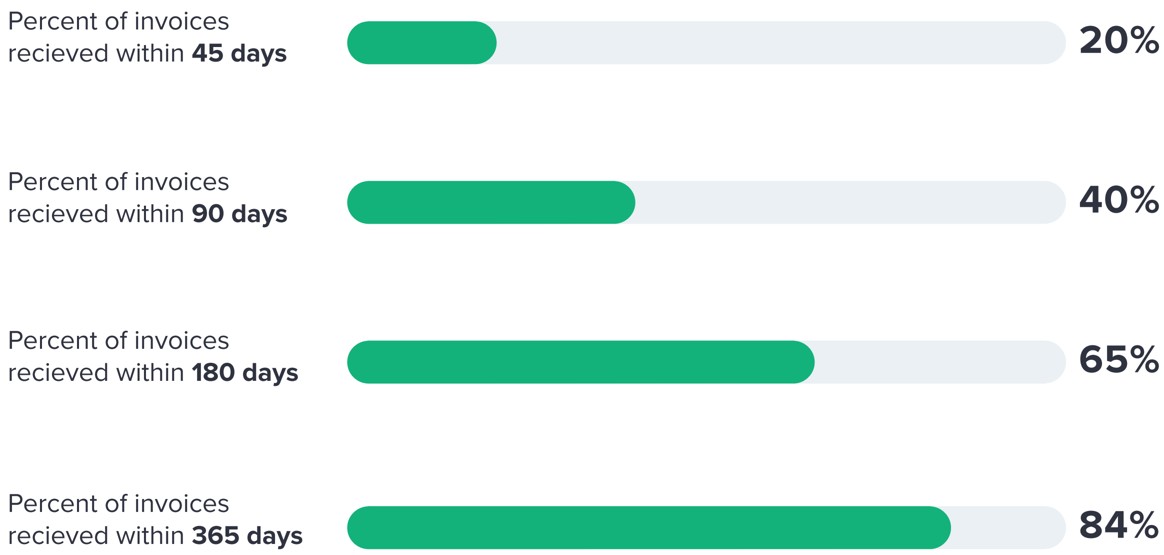
GENERAL

131 days
MEAN

78 days
MEDIAN

3.3 years
MAXIMUM

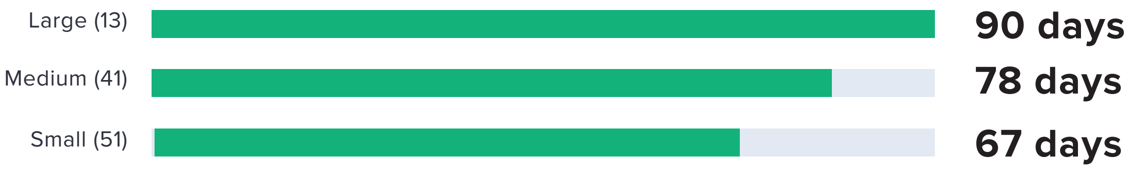
Invoices and duration



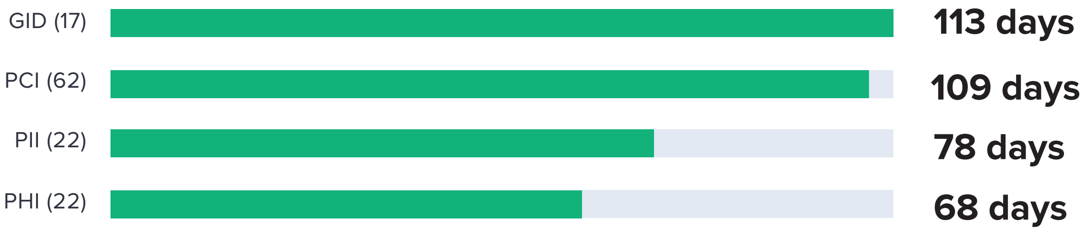
DURATION

Median duration

By size of the insured



By record type



Number of records versus duration

1 = High correlation
0 = No correlation

0.57

CORRELATION

Insights

The events within this section all involved costs, and the median duration was surprisingly low given that the breach events typically involved the engagement of multiple vendors. This fits with our experience. **Time is of the essence when dealing with breach matters.**

20% of invoice costs (or $88,800 of the mean cost) relating to breach events were issued within 45 days, **40%** (or $177,600 of the mean cost) were issued within 90 days. This highlights the important role of cyber insurance in maintaining cashflow, especially vital for small businesses.

While the tail for first party costs was short, this was not the case for third liabilities including **fines**.

The size of company has **no material impact on event duration.** This can be explained by the fact that legal requirements surrounding breach events are largely the same irrespective of company size.

It is surprising that the duration of events involving **PHI** records was the lowest. In our experience, the Office of Civil Rights (OCR) takes an active role in investigating these matters. However, **PHI** breaches below 500 records need not be reported to OCR and therefore the majority of breaches don't trigger an OCR investigation.

While there was some correlation between the size of breach and duration, the correlation is **not as strong as we might have anticipated.**

04

PANEL vs NON-PANEL

EVENTS

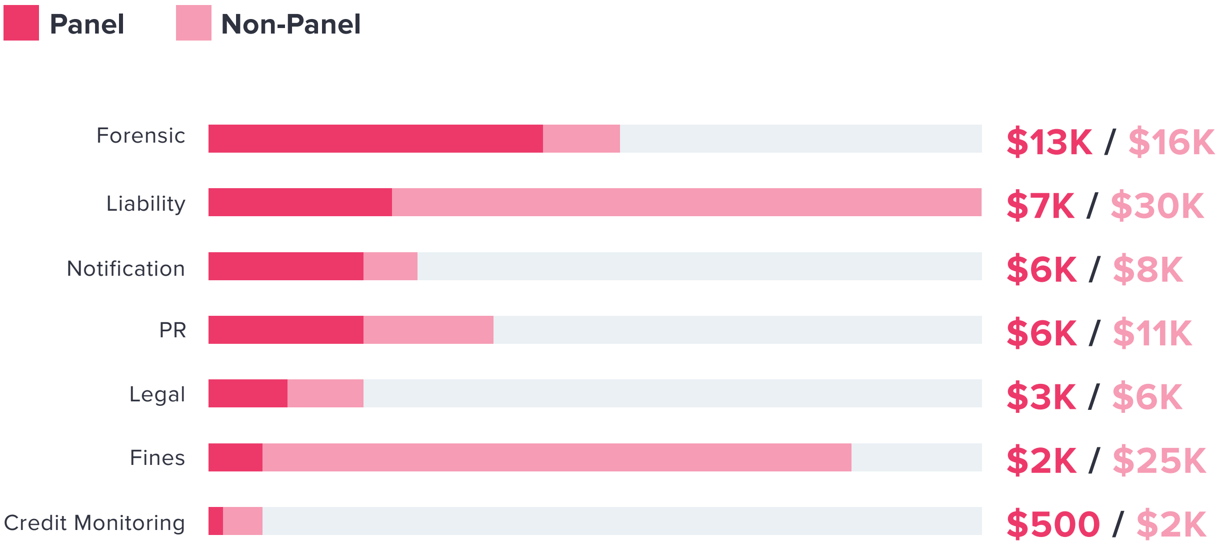
Panel vs Non-Panel

(for events with costs greater than zero)

Panel (129)	Non-Panel (45)
$16K **Median event cost** (where an event is panel if it has at least one panel cost)	**$25K** **Median event cost**
$29 **Median event cost** (per record)	**$44** **Median event cost** (per record)
300 **Median event size, in records** (includes zero cost events, unlike above)	**27** **Median event size, in records** (includes zero cost events, unlike above)

PANEL vs NON-PANEL

Median individual cost



Insights

The overall cost of breach events involving **panel** vendors ($19k) was 25% higher than **non-panel** ($14k). However, the **cost per record** of panel events ($29k) was half those of non-panel events ($60k). Accordingly, the benefit of using panel vendors on large breach events may be significant.

The largest drivers of cost savings for panel versus non-panel events were:

- **Credit Monitoring** ($500/$2k)
- **Legal** ($3k/$6k)
- **Public Relations** ($6k/$11k)