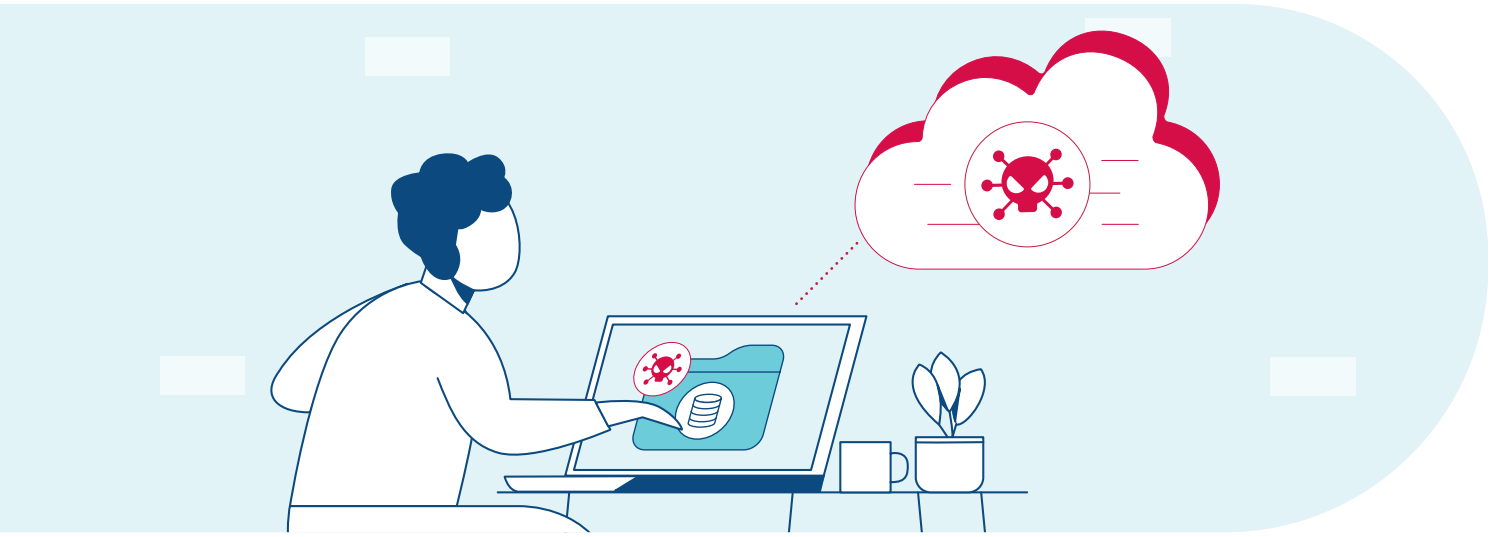
KROLL



Data Breach Outlook: Health Care is the Most Breached Industry of 2022

By David White,
Global Head of Breach Notification, Cyber Risk

Data breaches have become an unfortunate reality of the digital world we live in. While there is no doubt that efforts can be made to mitigate the chances of a data breach, living in a completely data breach-free world is not realistic. Apart from having processes and technology in place to prevent data breaches, companies should also have a plan of action in case they do suffer a breach.

One aspect of being prepared is understanding how vulnerable your industry may be to data breaches. Kroll handles thousands of incidents every year and in its Data Breach Outlook – Year in Review, it has ranked which industries continually top the charts.

Data Breaches Are Most Prolific in Health Care and Finance

In 2022, health care overtook finance as the most breached industry, accounting for 22% of the breaches handled by Kroll, compared to 16% in 2021; a 38% increase year over year. Finance dropped to second place with 19% of the cases in 2022, a 3% drop from 2021 where it accounted for 22% of breach cases.

Still in recovery from the pandemic, it is hardly surprising that the health care industry was particularly vulnerable to data breaches in 2022; at the very least, data management may have become less of a

priority, potentially putting data at risk of exposure. The finance industry continued to report a substantial number of breaches, likely because of the regulatory obligations in the industry which increase the amount of data breach disclosure. But, for a similar reason, it was surprising to see insurance slip out of the top five in 2022.

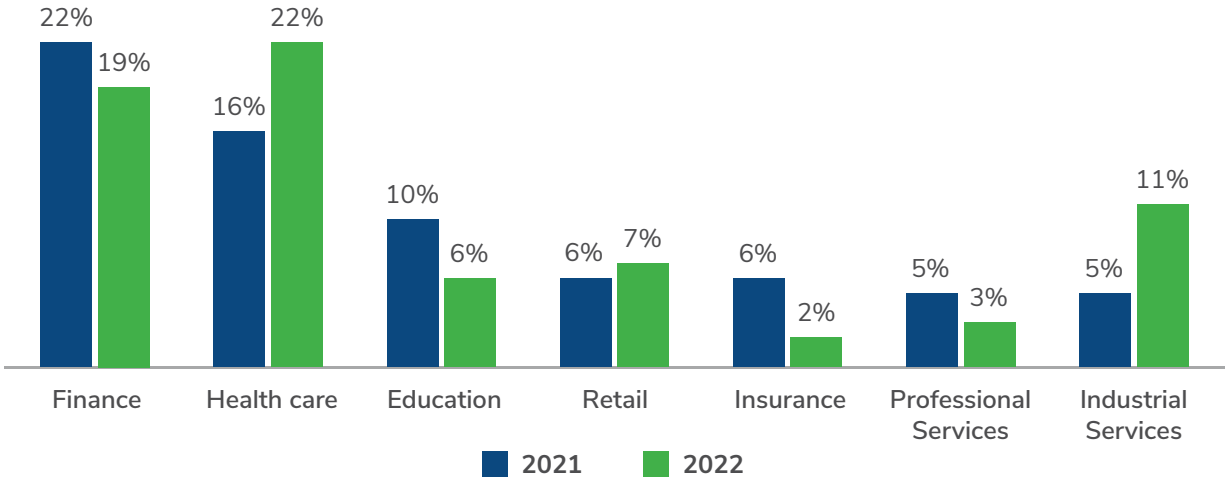
Shifts in Industrial Services, Not-for-Profit, Construction, Legal and Insurance

It was interesting to see the proportion of breaches hitting industrial services double in 2022. This points to a wider trend of industries which have previously considered the data they hold as "less sensitive," falling victim to data loss or cyberattacks, causing data compromise and consequently having to begin a notification process.

Other notable industry shifts in 2022:

- The industrial services industry doubled its proportion of cases from 5% in 2021 to 11%
- Both the not-for-profit and construction industries dropped out of the top 10 most-breached list
- The legal industry featured for the first time in the top 10 most-breached industries
- The proportion of breaches in the education industry fell from 10% of all cases in 2021 to 6% in 2022
- The insurance industry saw a smaller proportion of breaches than those in other sectors in 2022, accounting for only 2% of cases, compared to 6% in 2021

% of data breaches in 2021 vs 2022, by industry



Most Breached May Not Equate to Most Concerned Consumers

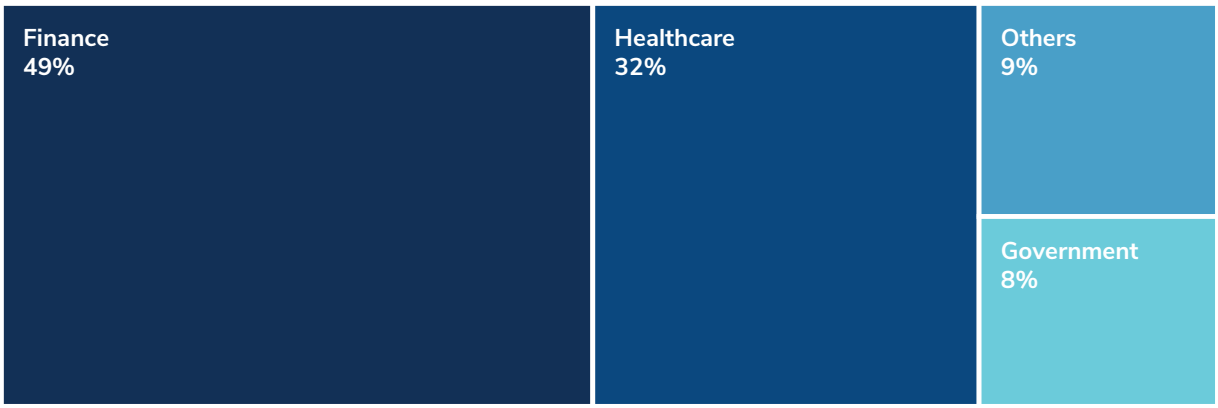
Further investigation into the data unveils some insights into how concerned consumers are in these respective industries about the data breaches in question. While health care may have suffered the largest proportion of incidents in 2022, the number of incoming calls related to these data breaches and the number of consumers which take up identity protection—often a combination of identity and credit monitoring—were still less than in the finance industry.

Findings include:

- Forty-nine percent of calls coming from consumers in 2022 following being notified of a breach were related to the finance industry, only 32% were in the health care industry
- Of all the monitoring taken up by consumers, 69% were involved in financial breaches, compared to only 20% in health care
- Finance saw a 127% year-on-year (YoY) increase in the number of calls following a breach; health care saw only a 19% increase
- Finance also saw a 126% YoY increase in the amount of identity monitoring taken up, compared to a 66% increase for consumers in health care

This potentially reveals that consumers are more concerned about their financial data than personal data related to health care. While in both industries personally identifiable information is at risk, given those looking to utilize this information—often cybercriminals—are largely perceived to be doing so for financial gain, it is understandable that financial data would be perceived to be more sensitive than health information. In reality, however, much of the data gathered from health care organizations—for example, social security numbers—could be used to set up fraudulent accounts and transactions. Concern is not misplaced, given the amount of revenue researchers believe is generated from this type of stolen data.

% of calls following data breaches in 2022



% of monitoring taken up following data breaches in 2022

It is possible to extrapolate the interpretation of this data further to indicate what organizations should perhaps be prepared for following a data breach. Perhaps the high number of calls and the take up of identity monitoring from the financial industry indicates that consumers are not only concerned about their data but potentially unhappy about how it has been managed. It may be wise for those organizations in the finance industry which suffer a breach to get prepared for litigation. Alternatively, it may show that the consumer support being provided by the finance industry is both accessible and necessary.

Understanding the drivers behind the *Data Breach Outlook* figures is subjective, and it is important that businesses combine this data with their own insight from talking to customers and market research. It is also true that while an industry may make up less of the overall number of data breach cases, it is not immune from the impact of a data breach and should similarly have playbooks if an incident was to occur.

This data may also be of interest to insurers looking to estimate the financial exposure of data breaches. A more engaged population of consumers impacted by a data breach could result in more identity monitoring and higher costs for the insurer and/or organization.

To understand more about how the data breach notification process works and what you can do ahead of time to ensure it runs as smoothly as possible with minimal financial and reputational damage, see this recent article on demystifying breach notification.

You may also be interested in reading our 2021 *Data Breach Outlook – 'Under-Attacked' Industries Feel the Heat*.

For more insights, visit the Cyber Blog at **kroll.com/cyberblog**

TALK TO A KROLL EXPERT TODAY

North America
T: 877 300 6816

UK
T: 808 101 2168

Hong Kong
T: 800 908 015

Additional hotlines at:
kroll.com/hotlines

Singapore
T: 800 101 3633

Australia
T: 1800 870 399

Brazil
T: 0800 761 2318

Or via email:
CyberResponse@kroll.com

About Kroll

As the leading independent provider of risk and financial advisory solutions, Kroll leverages our unique insights, data and technology to help clients stay ahead of complex demands. Kroll's global team continues the firm's nearly 100-year history of trusted expertise spanning risk, governance, transactions and valuation. Our advanced solutions and intelligence provide clients the foresight they need to create an enduring competitive advantage. At Kroll, our values define who we are and how we partner with clients and communities. Learn more at Kroll.com.