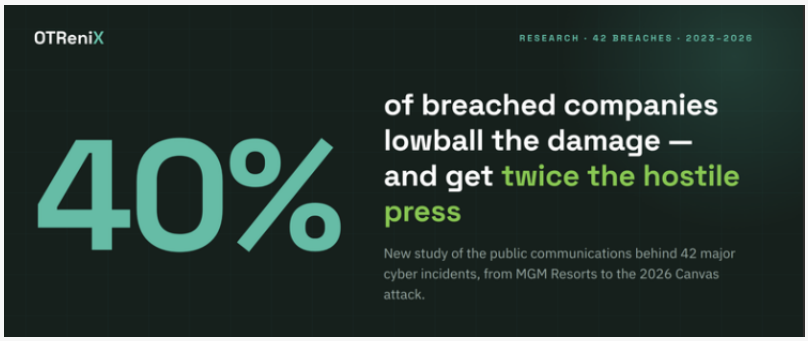
40% of Breached Companies Lowball the Damage and Get Twice the Hostile Press, OTReniX Study Finds

New research across 42 incidents, from MGM to the 2026 Canvas hack: 83% of first statements hide what was stolen, and 1 in 4 firms never name a victim count



NY, UNITED STATES, July 28, 2026 /EINPresswire.com/ -- Companies that understate the scale of a data breach in their first statement draw hostile media coverage twice as often as companies whose first numbers hold up 65% versus 32% according to a new study by OTReniX Cybersecurity marketing and PR firm. The agency tracked 42 major incidents disclosed between January 2023 and July 2026: what each company said first, when, how the numbers changed, and what followed.

> The press does not punish companies for being hacked - it punishes them for lowballing, stalling, and hiding”
>
> *Dmitrii Gavrikov, Fractional CMO*

Forty percent of the companies opened with a reassuring figure or a denial that later collapsed. Okta's "134 customers, about 1%" became every user of its support system. Change Healthcare went from no number to 190 million — the largest healthcare breach in US history. The UK's Co-op said there was "no evidence of data compromise" two days before hackers showed the stolen data to the BBC.

Key findings:

- 40% understated the damage, then corrected upward and drew hostile coverage in 65% of cases.
- 1 in 4 never said how many people were hit; journalists and hackers supplied the numbers instead.
- 83% opened with a euphemism "security incident" instead of naming what was stolen.
- The median company took 4 days to speak; 37% stayed silent for more than a week.

- 26% lost control of the story: attackers, journalists, or researchers broke the news first.
- Only 40% put a named executive in front of the story. Regular updates cut hostile coverage from 57% to 38%.

The companies that kept their reputation - Bybit, Coinbase, Qantas - all did the same three things: spoke fast, showed a face, and never stated as fact what they merely hoped.

The study also documents the failures: 23andMe telling victims the breach was "their fault" before filing for Chapter 11; Workday hiding its disclosure page from search engines with a "noindex" tag; Instructure declaring the 2026 Canvas incident "resolved" one day before attackers defaced 330 school login pages.

The disclosure window is also closing legally, the study notes: the SEC requires a filing within four business days of a materiality determination, GDPR gives 72 hours to notify regulators, and US state attorneys general run their own notification clocks. The median company in the sample spoke after 4 days; the average, dragged up by a long tail of silence, was 10.7 days.

The full report: https://otrenix.com/cybersecurity-pr-agency/#research

About OTReniX

OTReniX is a cybersecurity marketing and PR agency. We help infosec vendors earn visibility and trust: media relations, crisis communications, analyst relations, thought leadership, and full-stack marketing — locally and globally. More at otrenix.com.

Leo Schwarzebart
OTReniX
+1 315-202-9281
email us here
