ADRIANA VAN THO | GARRETT WADLEY | DANQING WANG

Data Analytics

→ Best Practices For Organizational Cyber Risk Management

Things to Discuss

Key goals:

- Exploring trends pre- and post-cyber breach
- Do better performers do anything unique to put them in this position?
- Are there industry differences?
- Reactivity to breaches

Methodology

Reading the data

We pulled the dataset into a csv, then analyzed it using python and Pandas.

Group data by relevant metrics

We grouped the data by the gvkey_hashed column, which represents individual companies. We also grouped by sic2 and sic3 when looking into individual industries.

Analyze the data

With our data read and grouped, we can begin looking into interesting trends and discovering insights.

Experiencing a cyber breach has an extreme effect on corporations' decisions to disclose.

Of all firms listed, companies average

56%

disclosure of their risks on their 10K annual report.

After a cyber breach, this number rises to over

88%

Top Disclosing Industries

Chemicals & Banking lead the way

With such high liability risks to customers, it's not hard to see why these industries would lead the way in risk disclosure.

Breach affects on 10K publishing – Risk

Breaches cause an upswing in some 1a keywords

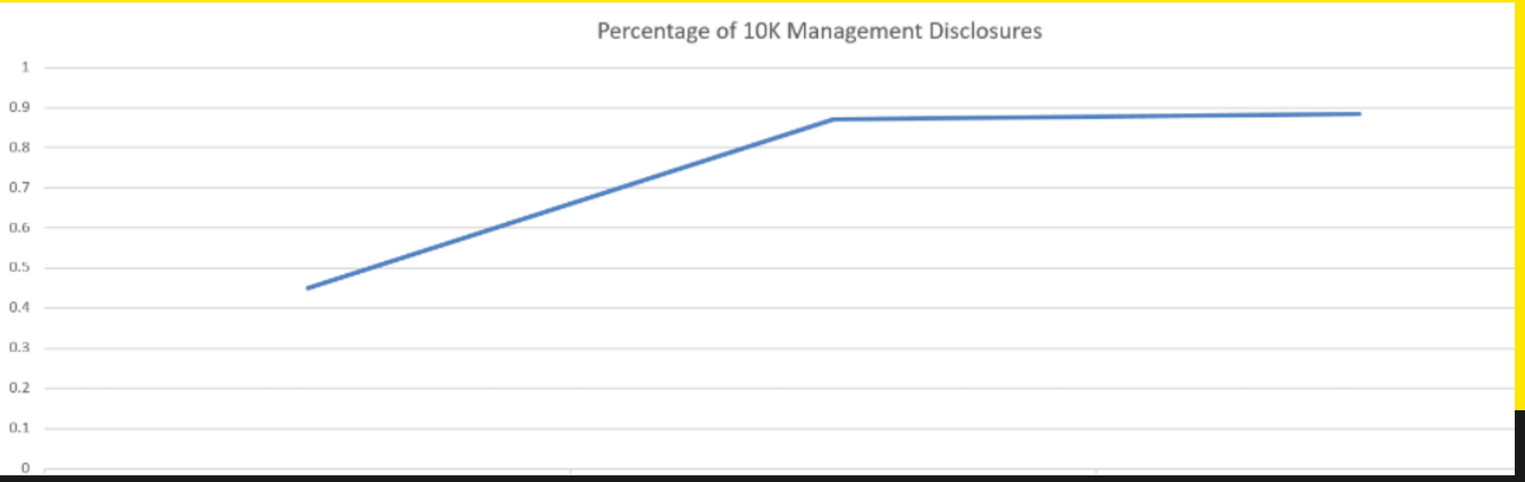
Once a breach happens, occurances on operational IT, Cybersecurity, and Risk Investment triple on average and are maintained at this level

Experiencing a cyber breach has a similar extreme effect on corporations' decisions to disclose its management strategies in tackling risks.

Of all firms listed, companies average

45%

disclosure of their management investment on their 10K annual report.



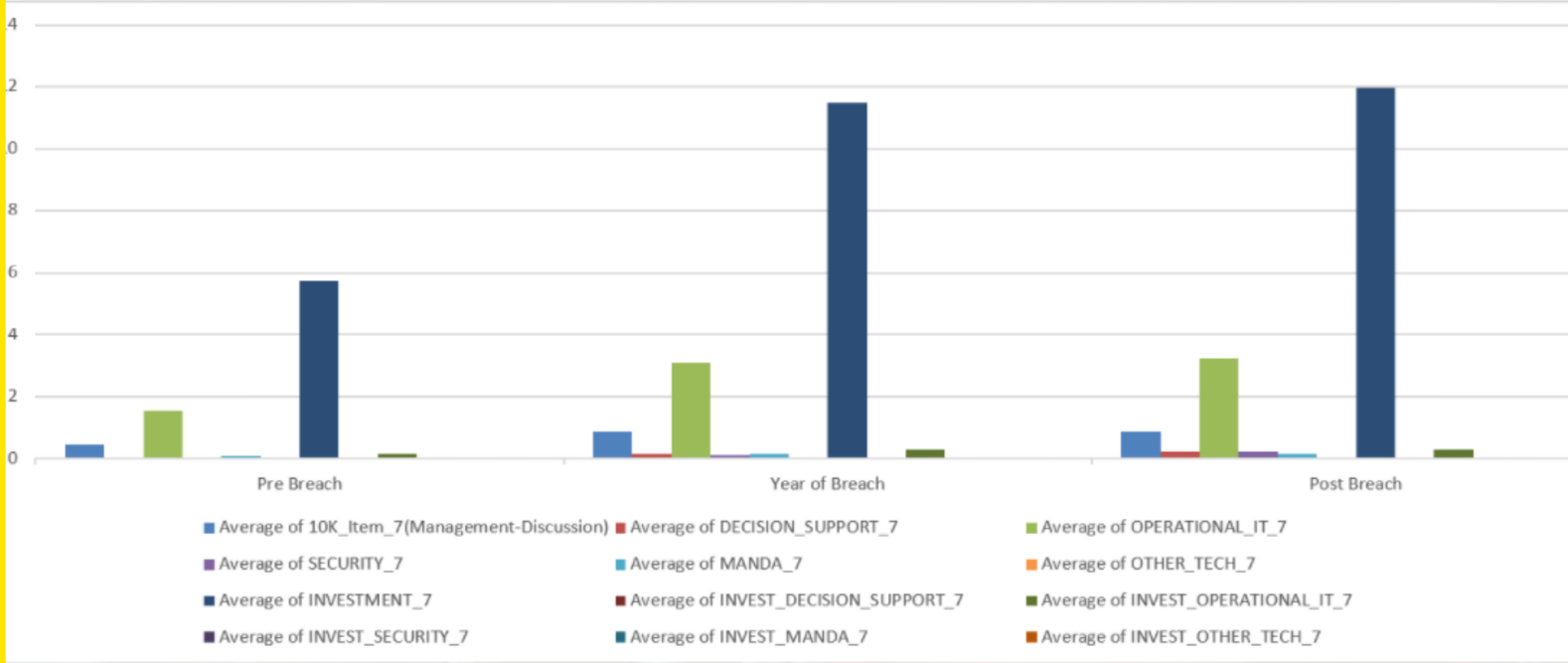
After a cyber breach, this number rises to over

88%

Breach effects on 10K – Management

Breaches cause a similar upswing in Item 7

Metrics also rise by about 200% on the 10K management side; most notable are Operational IT and Investment



Of breached firms,

12%

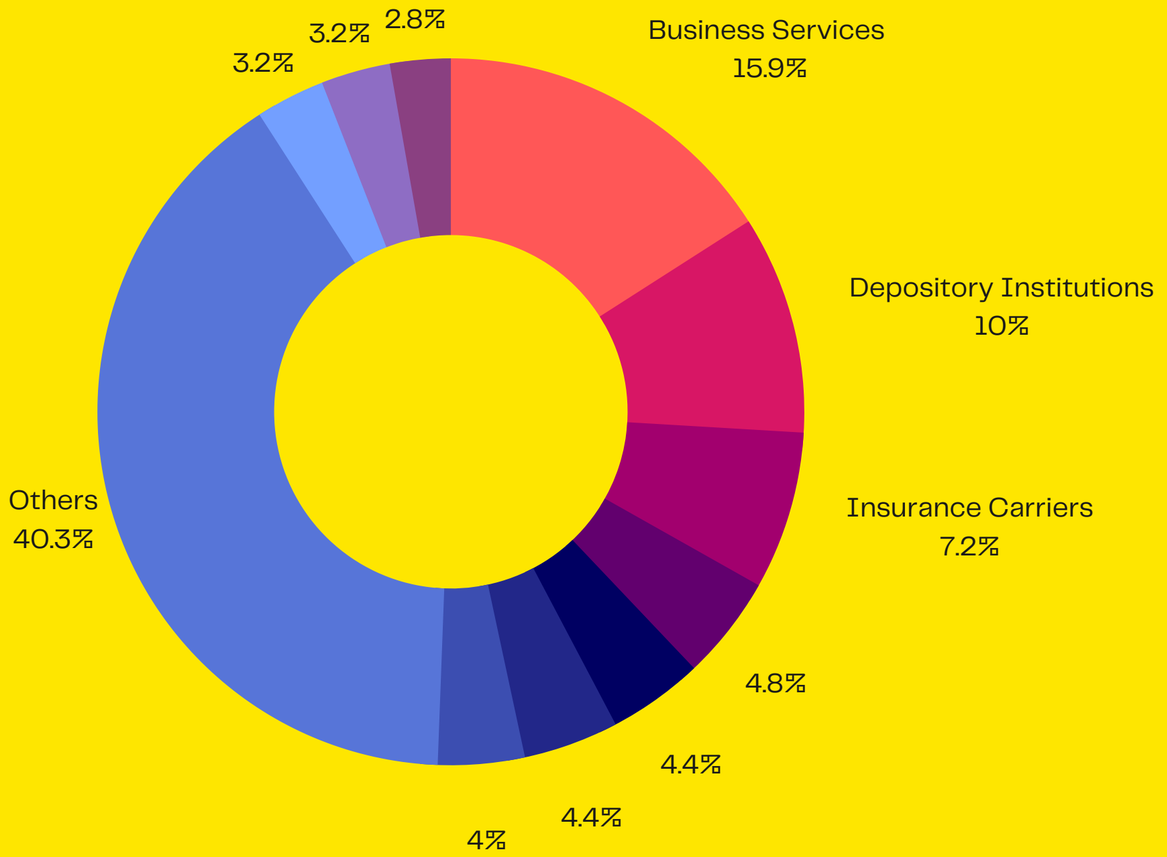
CANNOT pinpoint when a breach occurred.

Of these, insurance carriers were the most disproportionally affected. While most were submitting Risk Disclosures through 10Ks, less than half had mentions of Operational IT and Security prior to the breach.

Which industries detected the most breaches?

Top 3 most affected: Business Services, Depository Institutions, Insurance Carriers

Insurance carriers were the among the most disproportionate; while they discovered 7.3% of breaches, they account for only 2.7% of the firms on this list. Meanwhile, chemicals were among the best performers, despite being the third most common at 9.0%, they were low on the list of breaches with only 2.4%.



Breach Discovery Time

Savings Institutions and Misc. Business Services are slowest to discover

Most breaches that are discovered end up being found out almost immediately; much of these results beyond that are results of outliers. For example, Savings here had a breach that wasn't discovered for 8 years, while Business Services had a pair of them that took 2 and 6 years to find. Breaches are either quickly solved or deeply embedded in hidden layers.

Breach Announcement Time

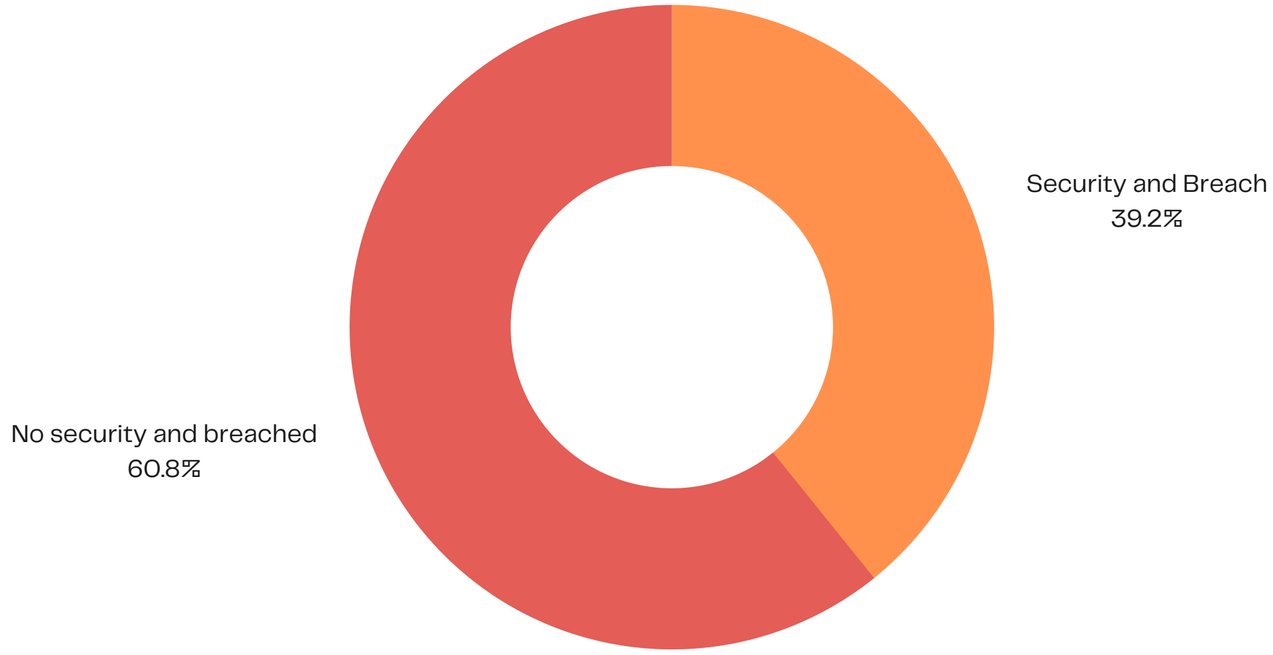
Atypical Results on Reporting

In industries not as intensely regulated as financial and accounting services that are typically targeted, there seems to be a slower time to announce breaches. This could be due to policy being less stringent, or simply that the blue-collar nature of some of these industries bay be concerned with maintaining status quo by putting off bad news to shareholders.

10K Risk Disclosure & Security R Effects on Likelihood of a Breach

Companies that posted mentions of Cybersecurity on their Risk 10K were less impacted

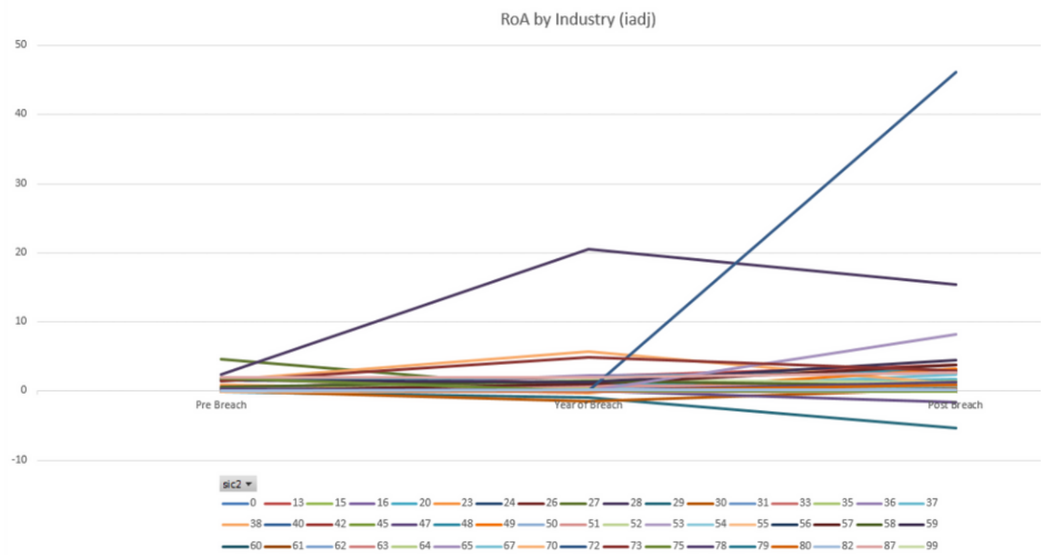
There were about 1.5 times the number of breaches to firms without any prior mentions of security on their 10K risk disclosure. While not a fool-proof statistic of measuring, there does seem to be a correlation to the results. Logic would have it that firms discussing the chances of attack are more ready to prevent them.

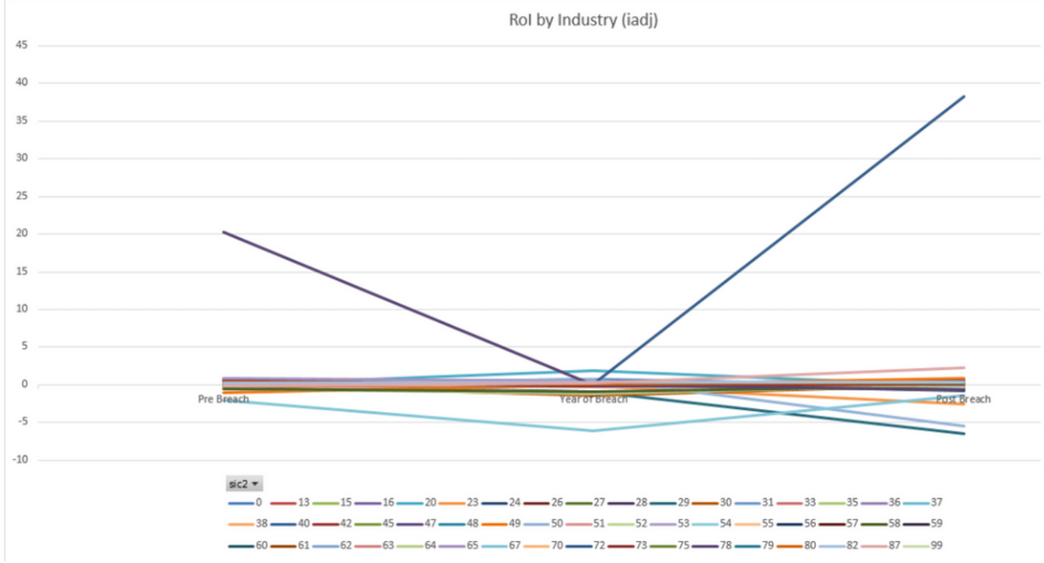


Breach Effects on Financial Performance

RoA and RoI share some similarities

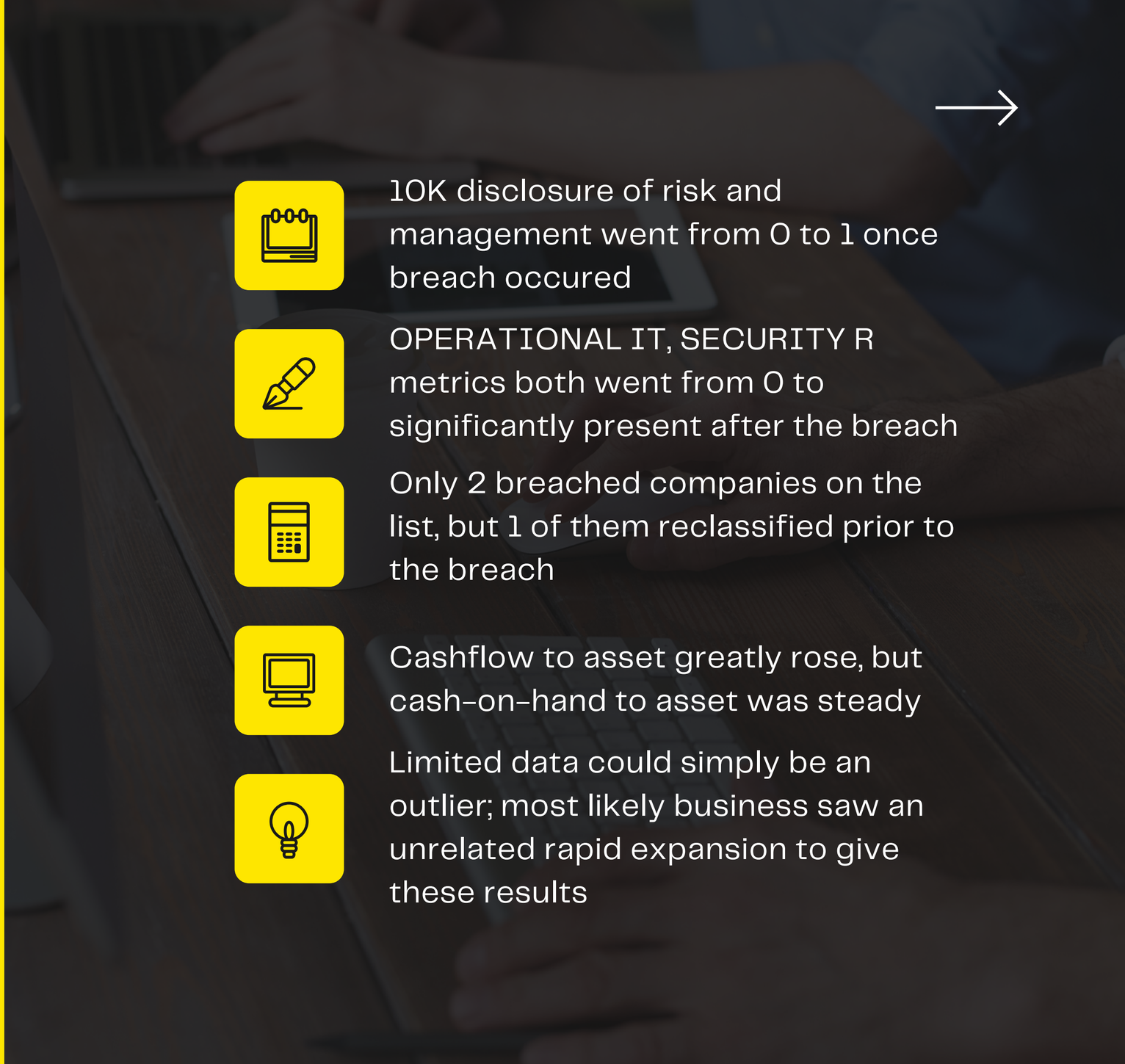
- 72 (Personal Services) is the big winner by both metrics
- 28 (Chemicals) goes from a top performer to bottom 10 by ROI, but dramatically improves through the breach by ROA
- 29 (Petroleum) is the biggest loser by both metrics
- Most are relatively stable, with downward trending after breach





Exploring Industry 72

Did laundromats and drycleaners really have the most prepared cybersecurity teams?



10K disclosure of risk and management went from 0 to 1 once breach occured

OPERATIONAL IT, SECURITY R metrics both went from 0 to significantly present after the breach

Only 2 breached companies on the list, but 1 of them reclassified prior to the breach

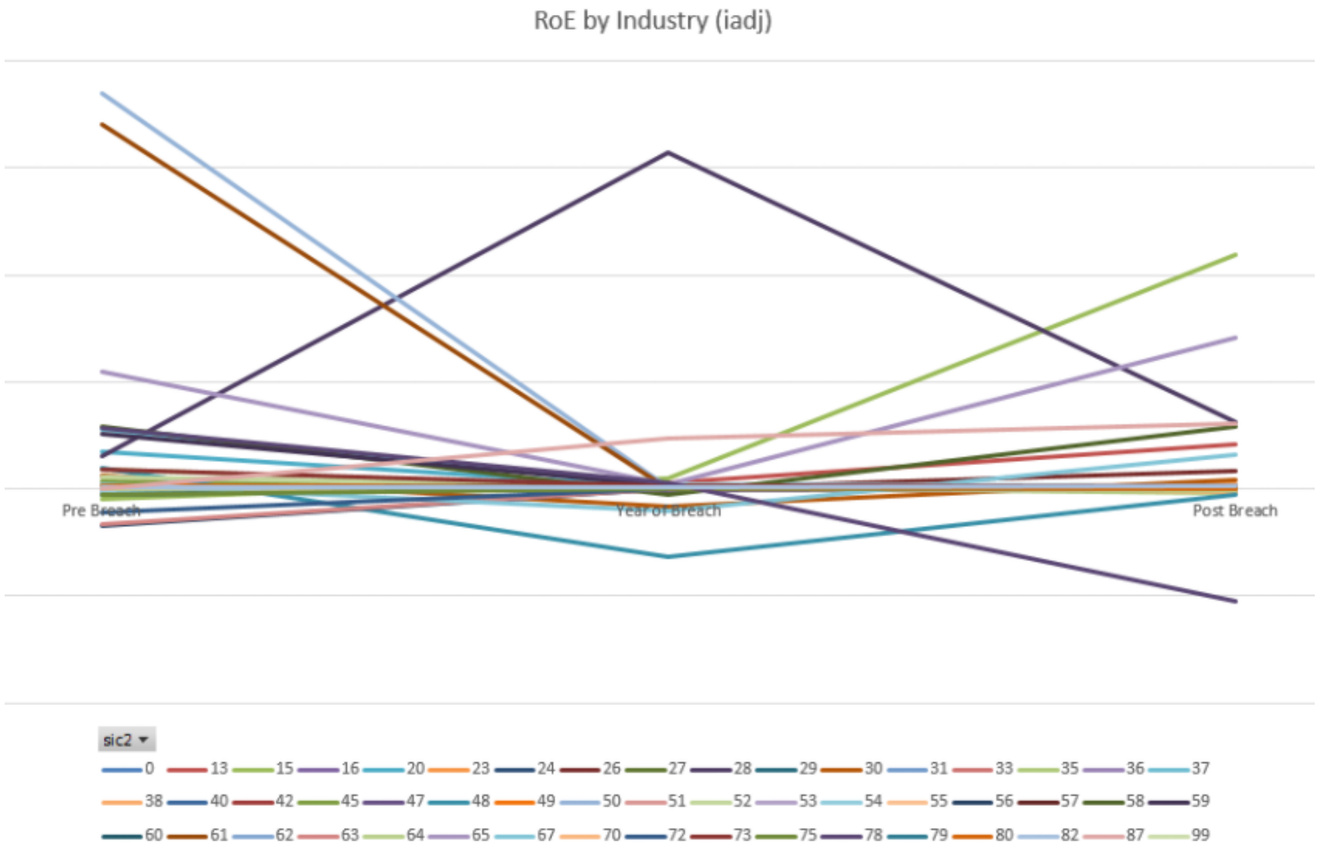
Cashflow to asset greatly rose, but cash-on-hand to asset was steady

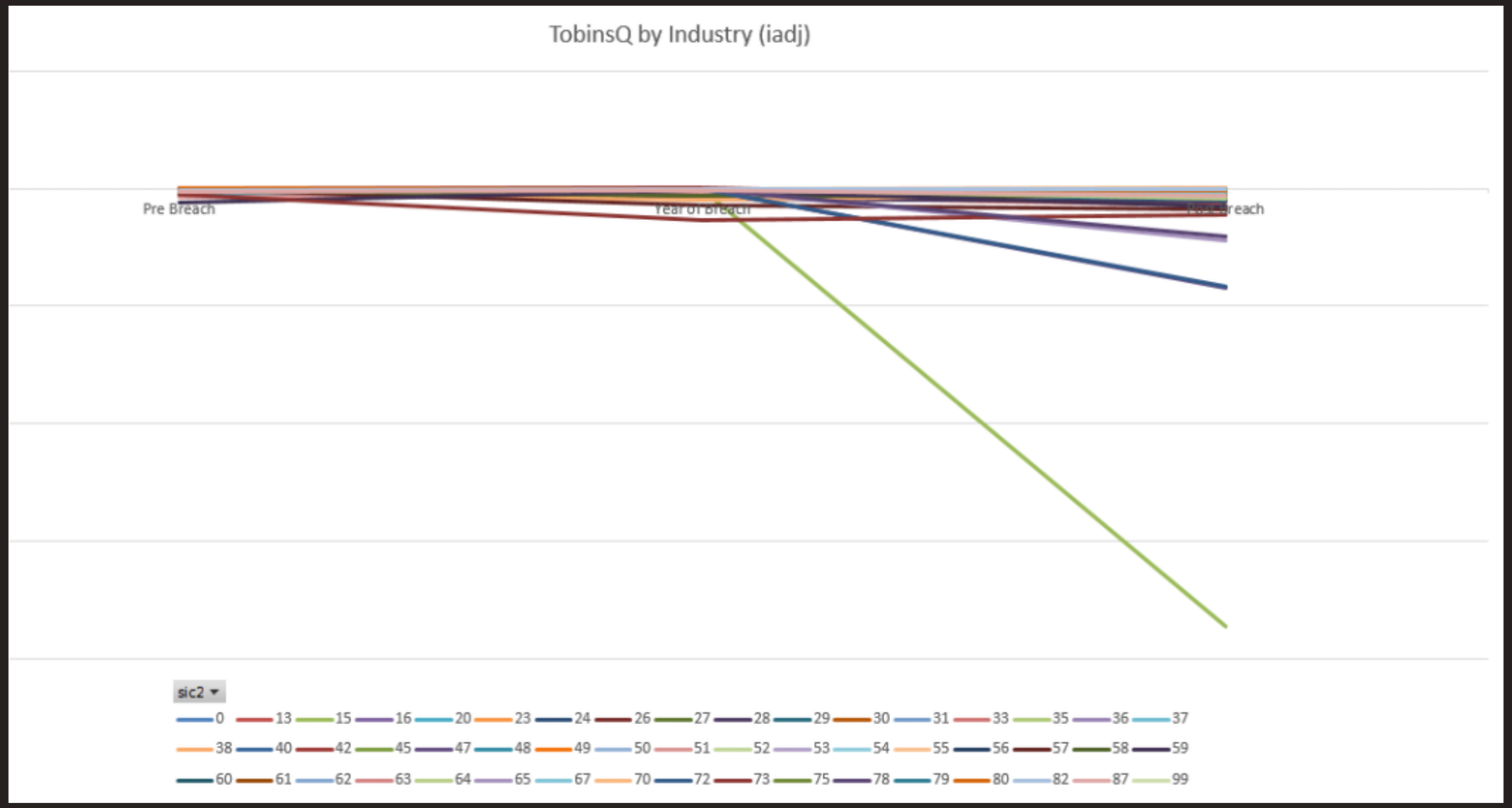
Limited data could simply be an outlier; most likely business saw an unrelated rapid expansion to give these results

ROE Effects

More varied results

- 28 (Chemicals) again appears with an interesting pattern; this time with it's greatest performance the year of the breach before regressing back to mean
- General wider variance in results before and after breaches; however, most industries seem general improvement after the breach under RoE
- Exceptions for 50 (Wholesale Goods) and 61 (Federal Credit Agencies) which had great performance prior to the breach but were deeply impacted.





TobinsQ

This metric clearly outputs a dramatically different – pessimistic – picture. No industry sees improvement after recovering from a breach, while some are heavily impacted.

Especially apparent here is industry 15 (General contractors & Builders), which by the other 3 metrics blended into the crowd as an average. Here. it is shown to have a massive downturn.

Our Recommendations

Always disclose

System to pinpoint when breaches occur

Business Services and Insurance Carriers need to improve their cybersecurity protections

NACD framework to assess those companies to have Board-level discussions

Budgeting risk investment planning, identify, and transform

Respond and recover using frameworks like NIST to reduce financial loss when breach occur

Whole sale, credit report, petrochemical

Prevent using SOCO to build better cybersecure environment and controls

Chemical, business service, banking

Thank You !

We'd love to respond to any questions you have.