The Institute of Internal Auditors Australia

CAE '60 Second' Survey

Protecting against Data and Privacy Breaches

November 2022

There have been a number of recent reports addressing theft of data and associated breaches of privacy. Some of these breaches have been associated with attempts at extortion. Most breaches affect smaller businesses but occasionally a major business is affected with resulting impact on a large number of people and significant adverse publicity (Webber Insurance Services, 2022).

The Institute of Internal Auditors – Australia surveyed Chief Audit Executives (CAEs) to explore the experience of Australian organisations in relation to data exposure and privacy breaches. 50 responses were received across a wide section of the economy (Exhibit 1). The CAEs of 45 (90%) organisations indicated that their organisations were subject to the Australian Privacy Principles (Office of the Australian Information Commissioner, n.d.). Two additional CAEs indicated that their organisation has elected to apply the principles within their organisation.

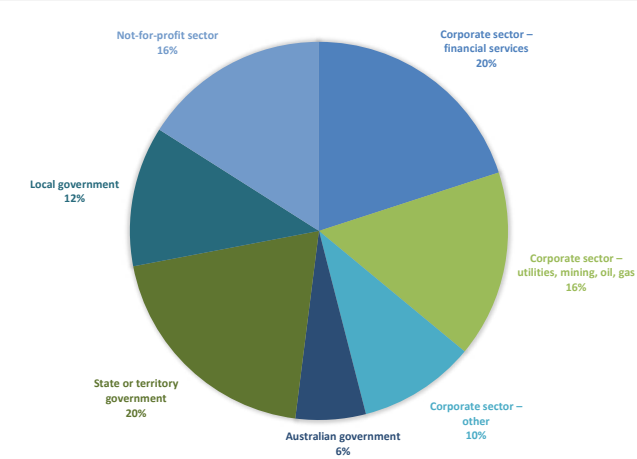

Exhibit 1 – Economic sector of respondents

For the purposes of this survey we defined:

- Data Breach – Unauthorised access to data from outside the organisation that compromises the confidentiality, integrity or availability of the data.
- Privacy – A fundamental right essential to autonomy and the protection of human dignity, serving as the foundation upon which many other human rights are built.

Of respondent organisations, 16 (32%) reported having experienced a data breach in the past 12 months, and 18 (36%) reported having had a privacy issue in the same period. Only one organisation reported having been subject to an extortion attempt.

Familiarity with Issues

All respondents reported some familiarity with the issues of data and privacy breaches. They tended to be more familiar with issues of privacy than with the specifics of data breaches (Exhibit 2).

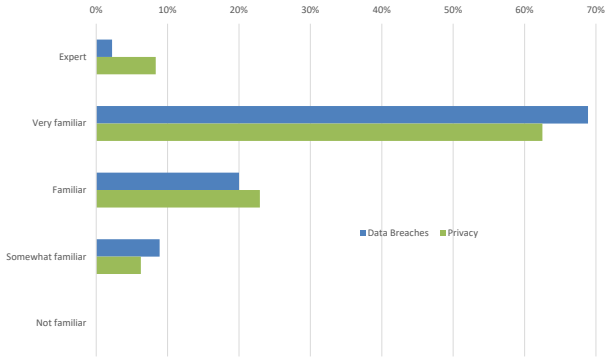

Exhibit 2 – Professed familiarity with relevant issues

Assurance

Monitoring and review (assurance) is an important component of any effective process. In a complex entity it is best if those responsible for delivery have more than one measure of its success. In many organisations this is expressed in the Three Lines Model (The Institute of Internal Auditors, Inc, 2020). 61% of relevant organisations reported having assurance over conformance with the Australian Privacy Principles; 22% of respondent CAEs were not sure of whether such assurance existed.

Where assurance was reported as being in place, it generally includes more than just internal audit, although internal audit assurance was most commonly used (Exhibit 3).

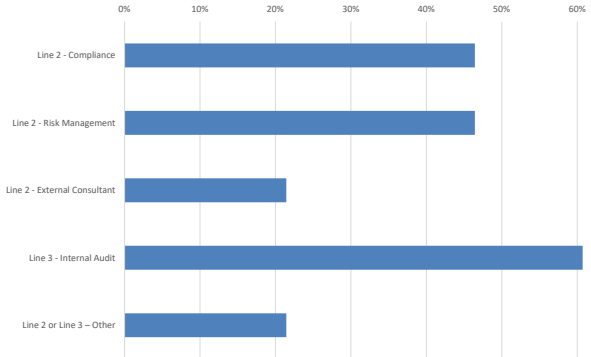

Exhibit 3 – Sources of assurance over conformance with Privacy Principles

Other sources of assurance reported include:

- (Line 2) accredited Information Security Management System (ISMS) auditor
- The organisation's legal team
- External reviews commissioned by Line 1
- Results of regulator review

Given the reliance on internal audit, it is surprising that 60% of organisations have not undertaken an internal audit of privacy management in the last 12 months. This is tempered to some degree by the observation that 18% of organisations have a review planned. (See Exhibit 4).

Cybersecurity has been regarded as a serious corporate risk for some time and it is therefore not surprising to observe that 76% of organisations have conducted an internal audit of cybersecurity within the past year (Exhibit 4).

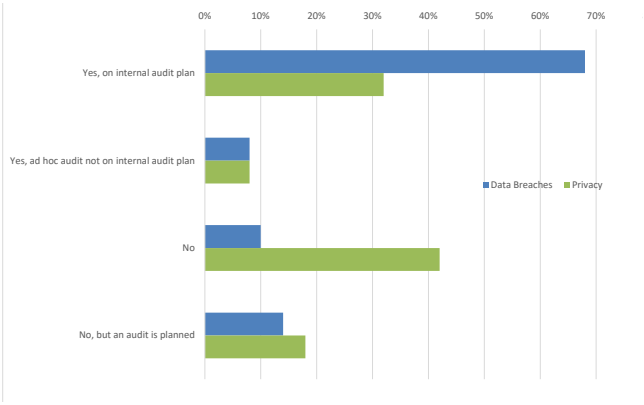

Exhibit 4 – Internal audit coverage

Heightened Measures

80% of organisations had recently heightened their assurance measures. Given recent events this is not surprising. We did not ask directly whether this was as a consequence of such events, nor did we investigate the reasons for organisations not enhancing their assurance. It is possible that organisations assessed their risk and decided that increased assurance was unnecessary. Indeed, some organisation indicated that they had long-standing uplift programs in place.

The range of additional measures (Exhibit 5) is similar to the range of existing assurance reported in Exhibit 3. While clearly there have been steps to enhance existing assurance mechanisms, the major initiative seems to be in obtaining additional external review.

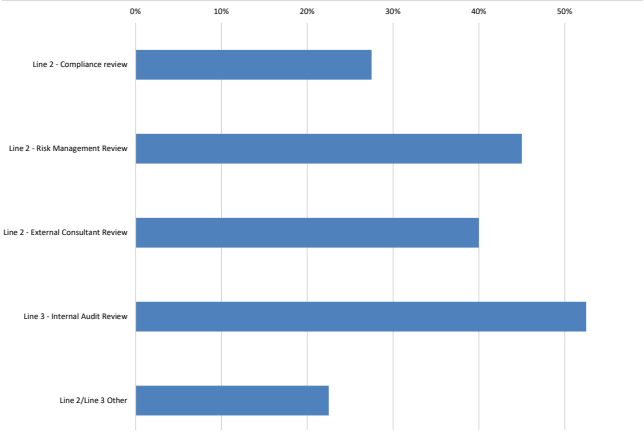

Exhibit 5 – Heightened assurance mechanisms

Summary

While there has been little reported in the way of attempted extortion against Australian organisations, it is clear that data breaches and privacy issues are relatively common. Organisations have responded to the threat by increased levels of assurance. While internal audit activity is still the most common form of assurance sought, there is an increasing use of Line 2 review resources.

Useful References

Austbrokers Countrywide, 2018. Top 10 Business Risks. [Online]
Available at: https://abcountrywide.com/top-10-business-risks/

Horne, S., 2021. White Paper: Cyber Risk Readiness, Response & Ransom: An Audit Committee Perspective. [Online]
Available at: https://iia.org.au/sf_docs/default-source/technical-resources/2018-whitepapers/iia-whitepaper_cyber-risk-readiness-response-and-ransom--an-audit-committee-perspective.pdf

Office of the Australian Information Commissioner, n.d. Australian Privacy Principles. [Online]
Available at: https://www.oaic.gov.au/privacy/australian-privacy-principles

The Institute of Internal Auditors - Australia, 2020. The 20 Critical Questions Series: What Directors should ask about Information and Cyber Security. [Online]
Available at: https://iia.org.au/sf_docs/default-source/technical-resources/20-critical-questions/20-questions-directors-should-ask-about-information-and-cyber-security.pdf

The Institute of Internal Auditors - Australia, 2020. The 20 Critical Questions Series: What Directors should ask about Information Management. [Online]
Available at: https://iia.org.au/sf_docs/default-source/technical-resources/20-critical-questions/20-questions-directors-should-ask-about-information-management.pdf

The Institute of Internal Auditors, Inc, 2020. The IIA's Three Lines Model: an update of the three lines of defense. [Online]
Available at: https://www.theiia.org/en/content/position-papers/2020/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense/

Webber Insurance Services, 2022. The Complete List of Data Breaches in Australia for 2018-2022. [Online]
Available at: https://www.webberinsurance.com.au/data-breaches-list