Making privacy core business

Data as nuclear fuel: both an asset and potential liability for organisations

22 March 2023

Privcore Pty Ltd

ACN: 167 388 178

ABN: 46 167 388 178

Email: operations@privcore.com

Website: www.privcore.com

Address: Level 14, 5 Martin Place, Sydney NSW 2000, Australia

Introduction

The information revolution that has fundamentally altered our society is fueled by data, particularly personal information, enabling significant efficiency gains and innovative solutions to problems. The benefits of handling data also pose risks of significant harms.[i] Whilst nuclear fission power plants use enriched uranium to generate electricity, their fuel is also capable of being used to construct nuclear weapons. Data is difficult to store safely for extended periods of time and privacy breaches are somewhat like nuclear meltdowns: uncertain in their timing and capable of radiating harms across significant proportions of the population for an extended period of time.

Whilst enriched uranium nuclear power plants are highly regulated with a significant investment in safety and security (and even banned in some countries), cyber security and privacy regulation has been slower to keep pace with the growing harms resulting from the mis-use of data. Many factors have been argued to contribute to this problem, including surveillance capitalism[ii], incentives encouraging startups to release insecure minimum viable products[iii], and contracts which limit the extent to which software developers are liable for harm[iv], etc.

Governments and industry regulators have responded to the risks of harms from cyber-attacks and privacy breaches through an array of strengthened regulations. In Australia, we have privacy legislation at the federal level and in most states/territories, sectoral regulation like APRA's CPS 234 and CPS 230, directors' duties under the Corporations Act, the Security of Critical Infrastructure Act, ASX Listing Rules requiring disclosure of market sensitive information, and proposals for a Cyber Security Act (amongst others). Similar, or stronger, regulatory regimes exist or are under development in many comparable jurisdictions.

Whilst most of these laws, codes and regulations seek to incentivize uplift in organisations' cyber security and privacy maturity through threats of post-breach sanctions, evidence suggests that many government agencies and the private sector are still under-investing in cyber security and privacy controls.[v] One contributing factor to this under-investment is the failure to account for externalities when making cyber security and privacy control funding decisions (such as in the original (still widely-used) Gordon-Loeb 2002 model for calculating cyber security investments).[vi]

"convincing the CFO to increase the budget for cybersecurity activities often becomes more of an art than a science"[vii]

Reactive regulation is not the only way to alter the decisions made by organisational leaders. Proactive regulation which incentivises organisations to uplift their cyber security and privacy maturity on a regular basis regardless of whether a breach has occurred is another option, which arguably has received less attention from scholars, government and industry experts.

This whitepaper is an initial attempt to draw attention to how improving current accounting standards creates an additional (proactive) regulatory tool to drive uplift in organisations' cyber security and privacy maturity. It identifies:

a) a number of challenges in existing accounting standards which contribute to the incentives driving current under-investment; and

b) an opportunity for cyber security and privacy industry experts to engage with accounting standards bodies to drive uplift in organisations' cyber security and privacy maturity.

How do current accounting standards hinder cyber security and privacy maturity uplift?

Cyber security and privacy are not the main focus of accounting standards and financial reporting – which is to enable investors and creditors to more accurately understand how organisations are performing, and to make better decisions regarding those organisations. Whilst accountants do not deal with concepts like Internet Protocols and Zero-Days, they do have their own technical language and formalized processes to create and alter rules for how organisations' accounts are prepared and disclosed. Unlike hackers, accountants operate on periodic time cycles, focusing on concepts like assets, liabilities, expenses, revenue and capital, so it is appropriate to explore how the problems identified in the previous section have been influenced by the way accountants think about some of those concepts.

a) Assets:

It is obvious that physical things like buildings and production lines can be tangible assets of organisations. As the Information Age has progressed over the last few decades, intangible assets (such as software licences) have become critically important to increasing the productivity and value of organisations.[viii] For much of the Information Age, accounting standards made a distinction between whether different types of intangible assets could be recognised on the balance sheet of an organisation. Whilst intangible assets that were purchased from third parties could be recognised as an asset, internally-developed intangible assets could not. This has only relatively recently changed to permit recognition on the balance sheet of internally generated intangible assets.[ix]

"many highly valuable internally generated intangible assets remain unrecognized and undisclosed in financial statements" [x]

One of the interesting consequences of this accounting decision is its impact on data mining, cyber security and privacy. For example, when companies listed on the stock exchange that took advantage of Big Data analytics did not have to inform their investors or lenders about the size or value of the datasets of personal information which they were holding, a gap widened between the book value of their assets and their total market capitalization (accountants refer to this broader issue as the "asset-light" problem). Those organisations could build massive internal datasets containing billions of records and inferences about tens of millions of people but not have to list those datasets as assets on their balance sheet.

"this suggests that financial statements do not adequately reflect the underlying economic substance of entities"[xi]

Information that is hidden from disclosure in financial reports affects not just the decision-making of external parties like investors and lenders. It also influences the decision-making of internal parties within organisations, notably their boards and executives. Their decisions about the necessary maturity of data governance programs, and appropriate investments into cyber security and privacy controls are affected.

Without the pressure of adequate transparency required by financial reporting rules, organisations have a natural tendency to under-invest in uplifting their cyber security and privacy maturity, often preferring to deliver a mix of greater profits to their owners and greater bonuses to their leadership.[xii] The expenses necessary to achieve that maturity uplift are certain to lower bottom-line profits (and potentially bonuses) in the short term whilst the benefits of increased cyber security and privacy maturity are less certain and longer-term (if an organisation is not the victim of a successful cyber-attack or data breach, was that because of the adequacy of its existing controls? or because it was not targeted that year?).

"respondents do not consider financial statements prepared in accordance with AASB138 to be useful relative to other sources of information about unrecognized internally generated intangible assets"[xiii]

Whilst the challenges in valuing intangible assets like data lakes of personal information and inferences generated from data analytics has been used as a justification by some organisations to not report those assets on their balance sheets[xiv], there is a situation in which such datasets have come to be routinely valued. When organisations enter bankruptcy in the USA, customer datasets are valued and sold as valuable assets to third parties (typically operating in a similar line of business) to help pay off outstanding creditors of that organisation. The American Bankruptcy Code and bankruptcy courts have even utilized the role of a "consumer privacy ombudsman" who expertly assesses whether the proposed sale might create excessive privacy harms.[xv]

b) Liabilities:

Beyond the asset side of the balance sheet, another issue that exacerbates the lack of disclosure in financial reports about high-risk datasets containing large volumes of personal information is the way in which accountants interpret some liabilities as either provisions (which are reported and affect bottom line profits) or contingent liabilities (which are disclosed, but which do not affect bottom line profits).[xvi]

"investors & creditors need to be able to accurately assess… management's stewardship [and prospects for future cash flows]" [xvii]

For example, organisations currently only report as provisions in their balance sheets direct costs expected to be incurred because of data breaches that have already occurred (financial reports are backwards looking in time).[xviii] The costs of compensating potential litigation by victims of data breaches might be disclosed as a contingent liability, but do not affect

profitability during the time period in which the data breach occurred. The much larger indirect costs typically incurred by organisations after a data breach (such as reputation loss, distracted executives, reduced future sales, etc.) are not typically reported or disclosed at the time of a data breach, except perhaps as expenses causing a subsequent earnings downgrade which may or may not be linked by the organisation to the data breach.[xix]

c) Reporting time cycles:

The annual cycle and historical focus of financial reporting under accounting standards may also contribute to under-investment in cyber security and privacy controls.[xx] Hackers tend to be unpredictable, and the time taken to detect and respond to a data breach is often lengthy. This means that many data breaches straddle across financial reporting periods (i.e. the hackers penetrated the organisation's systems during one accounting period, detection occurred in the next financial period and the consequences of the breach (particularly indirect costs) will continue to affect the organisation over the next several accounting periods). Therefore, any one financial report will only contain a partial view of the overall data breach and its consequences – profits may be over-stated in one financial report because costs will be incurred in subsequent years. Inherent uncertainties in data breach consequences intersect with limitations on how organisations can report provisions and disclose contingent liabilities, making it harder for investors and lenders to get an accurate understanding of how well the organisation is adequately investing to control its cyber security and privacy risks.[xxi]

"Uncertainty is a form of risk for a firm"[xxii]

d) Materiality:

Underlying analysis of both assets and liabilities (and revenue/expenses) is the accounting concept of materiality.[xxiii] It acts as a high-pass filter, enabling an organisation to ignore (for financial reporting purposes) amounts considered to be too small relative to the size of the organisation. Until recently in Australia, many more organisations than you might expect could regard a data breach as being more likely to be immaterial than material. This was due to the Privacy Act 1988 (Cth) excluding from compliance most businesses with less than $3 million in annual turnover (the small business exemption), the low level of penalties and enforcement under that Act, and the limited means for victims of data breaches to seek a remedy. However, given:

a) the recent amendments to the Privacy Act which significantly increase penalties for interferences with privacy; and
b) the Attorney-General's Department's recommendations to remove the small business exemption and introduce both a direct right of action and statutory tort;

organisations will need to re-assess the extent to which they regard interferences with privacy as material from an accounting perspective. This includes interferences with privacy beyond data breaches.

Opportunities to influence new accounting standards on cyber security and privacy

Both Australian and international accounting standards bodies are in the early stages of a lengthy process to consider how cyber security and privacy risks affect the information communicated to investors and lenders through financial reports (falling within the accounting concept of sustainability).[xxiv] This provides an opportunity for Australia's cyber security and privacy expert communities to help influence and shape the extent to which another regulatory regime motivates organisations to uplift their cyber security and privacy postures.

Unlike the reactive nature of the notifiable data breaches scheme and increased penalty provisions under the Privacy Act, one advantage of financial reporting obligations and accounting standards is that they can proactively influence organisational behaviour (i.e. organisations have to prepare and publish annual financial reports, regardless of whether or not they have experienced a data breach that year). This means that increased cyber security and privacy reporting obligations imposed by accounting standards have the potential to apply consistent prospective pressure on organisations to uplift their cyber security and privacy maturities systematically, rather than the sporadic pressures imposed when organisations are recovering from a data breach.

Just as cyber security and privacy experts benefit from the help of accountants when preparing their tax returns, accountants are likely to benefit from the insights of cyber security and privacy experts when developing and revising accounting standards relevant to cyber security and privacy. The first challenge in achieving the benefits possible from such a collaboration is for both groups of experts to better understand each other's concepts and jargon. The second is to gain the capability to successfully navigate each other's institutional processes. Patience is the third challenge – new accounting standards are not developed overnight. Indeed, they may take five to ten years – which is several generations of risk evolution in cyber security terms.

Sustained effective engagement with the development of accounting standards relevant to cyber security and privacy will likely require the involvement of and support from both industry bodies, (such as the Australian Information Security Association, ISACA, and ISC2) and government agencies (such as the ACSC, staff of the Minister for Cyber Security, and DFAT's Ambassador for Cyber Affairs and Critical Technologies). Failure to engage effectively may result in the development of accounting standards and financial reporting requirements in Australia and internationally which undermine incentives for organisations to invest in uplifting their cyber security and privacy maturities.

Conclusion

Experiences with cyber-attacks and privacy breaches over the last decade have highlighted the dual-nature of data, capable of simultaneously fueling the Information Age and causing significant harm when mis-used or leaked. As under-investment by organisations in uplifting

their cyber security and privacy maturity persists despite implementation of many reactive regulatory regimes. This White Paper explores the potential for how proactive regulation via changes to accounting standards might reduce the extent to which data continues to leak from organisations as a form of toxic waste. It has identified an opportunity for Australia's cyber security and privacy expert communities to begin a conversation with accounting standards bodies to assist them to craft new accounting standards which may drive organisations to make more adequate investments into uplifting their cyber security and privacy maturity.

About the author

Dr John Selby, CISSP, CISM, FIP, CIPM, CIPP/E, Senior Consultant and Head of Research at Privcore consults to governments, large technology companies and startups on strategic privacy, artificial intelligence and cyber security governance risks. He works with clients on cybersecurity and privacy in ways that capture his audience's attention and garners action. Clients appreciate that he can express complex cybersecurity, AI and privacy issues in ways that resonate and make sense to them.

Dr Selby is the author of one of the seminal articles on data localisation, and has spoken on cyber security, privacy and AI issues at numerous forums around the world, including the United Nations Internet Governance Forum, the Australian Institute of Company Directors, AISA's CyberCon and IAPP's ANZ Summit. He has been interviewed by Channel 7 and 9 news, Weekend Sunrise, The Project, the Sydney Morning Herald, the Australian Financial Review, ABC Radio and The Conversation. The Lowy Institute named him as one of Australia's "New Voices in Technology and International Relations" in 2006.

Prior to joining Privcore, he developed and taught privacy, AI and cyber security governance and law courses at Macquarie University. He received an iappANZ Legacy Grant for privacy. Dr Selby led the SIMProtect project <simprotect.org.au> to increase awareness of identity theft and financial fraud risks for tens of thousands of Australians, which was a finalist for the AISA 2021 Cyber Security Outreach Program of the Year.

About Privcore

Privcore's team with over 40 years' combined experience helps business and government make privacy core business, so they can deliver services with the trust and confidence of customers and citizens. Privcore conducts privacy impact assessments, privacy health checks or audits, data breach prevention and recovery, privacy by design, builds privacy programs, provides advice, policies and conducts research into privacy and cybersecurity.

Please note that Privcore provides privacy risk management advice, not legal advice.

[i] Cory Doctorow, 'Personal Data is as Hot as Nuclear Waste' *The Guardian* (16 January 2008)
[ii] Shoshana Zuboff, 'The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power' (2017) Ingram Publisher Services
[iii] Ron Zalkind and Tsahy Shapsa, 'What is Minimum Viable Security (MVS)? *Open View Partners Blog* (15 February 2022)
[iv] David Sanger, 'New Biden Cybersecurity Strategy Assigns Responsibility to Tech Firms' *The New York Times* (2 March 2023)
[v] The audit offices of Commonwealth and state governments have repeatedly lamented the inability of agencies to fully implement even the ASD's "Essential Eight" controls. For analysis of the private sector's incentives to under-invest in adequate controls, see: Lawrence Gordon, et al, 'Empirical Evidence on the Determinants of Cybersecurity Investments in Private Sector Firms' (2018) 9 *Journal of Information Security* 133-153
[vi] Gordon, et al admitted in a 2015 article that their original model facilitated private sector firms' decisions to under-invest in cyber security controls due to its failure to account for externalities. Depending upon the ratio of the externalities to the internal losses to the organisation, such under-investment could be substantial: Lawrence Gordon, et al, 'Externalities and the Magnitude of Cyber Security Underinvestment by Private-Sector Firms: A Modification of the Gordon-Loeb Model' (2015) 6 *Journal of Information Security* 24-30
[vii] Lawrence Gordon, et al 'Empirical Evidence on the Determinants of Cybersecurity Investments in Private Sector Firms' (2018) 9 *Journal of Information Security* 133
[viii] Australian Accounting Standards Board, Australian Accounting Standard AASB138 Intangible Assets
[ix] Not all accountants agree with this change: see, for example, Stephen Penman, Accounting for Intangible Assets: Thinking It Through (2023) *Australian Accounting Review* (forthcoming)
[x] Australian Accounting Standards Board, Staff Paper: Intangible Assets: Reducing the Financial Statements Information Gap Through Improved Disclosures (March 2022) p5
[xi] Ibid, p6
[xii] Lawrence Gordon, et al 'Empirical Evidence on the Determinants of Cybersecurity Investments in Private Sector Firms' (2018) 9 *Journal of Information Security* 133
[xiii] Australian Accounting Standards Board, Staff Paper: Intangible Assets: Reducing the Financial Statements Information Gap Through Improved Disclosures (March 2022), p14
[xiv] Laura Veldkamp, 'Valuing Data as an Asset' (2023) *Review of Finance* 1-18; Jurgen Sidgman and Malcolm Crompton, 'Valuing Personal Information to Foster Privacy: A Thought Experiment and Opportunities for Research' (2016) 30(2) *Journal of Information Systems* 169-181
[xv] Michael Brandess and Kathryn Nadro, 'Getting Personal: Acquiring PII out of Bankruptcy' (2022) 41 *American Bankruptcy Institute Journal* 14
[xvi] Australian Accounting Standards Board, AASB Standard 137: Provisions, Contingent Liabilities and Contingent Assets; Australian Auditing and Assurance Standards Board, Staff Paper: The Consideration of Cyber Security Risks in an Audit of a Financial Report (May 2021)
[xvii] International Accounting Standards Board, Conceptual Framework for Financial Reporting, paragraph 1.3.
[xviii] See, for example, how Medibank Private disclosed provisions for direct costs arising out of its 2022 data breach in its financial reports.
[xix] Marty Puranik, 'What is the Cost of a Data Breach?' *Forbes* (2 December 2019)
[xx] Australian Auditing and Assurance Standards Board, Staff Paper: The Consideration of Cyber Security Risks in an Audit of a Financial Report (May 2021)
[xxi] Australian Auditing and Assurance Standards Board, Staff Paper: The Consideration of Cyber Security Risks in an Audit of a Financial Report (May 2021)
[xxii] Professor Laura Veldkamp 'Valuing Data and Data-Intensive Firms' *Keynote Speech to the 49th Meeting of the European Finance Association* (14 October 2022)
[xxiii] Australian Accounting Standards Board, *Practice Statement: Making Materiality Judgements* (December 2021)
[xxiv] Australian Accounting Standards Board, Staff Paper: Project: Sustainability Reporting GSSB Draft Work Program 2023-2025 (23 January 2023), paragraphs 13-15; IFRS, Staff Paper: Management Commentary Risks (May 2020)