News release: Sunday, 19 August 2018

Expert Analysis Finds 14 Recent Cyber Breaches Average a 'D minus' on Disclosure

"Like watching a slow-motion governance train wreck." Peter Coroneos, co-author

According to the authors of the just published *Cyber Breach Communication Playbook*, 14 recent major cyber breaches affecting Australian and international organisations just managed to avoid a fail average in the way they handled post breach communication.

They found that consequences of the mishandling ranged from senior executive resignations, parliamentary inquiries, loss of customers, significant share price, revenue and business valuation reductions, litigation, damages and compensation orders and general lingering brand damage from an increasingly distrustful public.

"Systemic failures are adding to fears that information is not longer safe even in the hands of major brands or government databases", said Peter Coroneos, cyber industry leader and book co-author. "It borders on inexcusable that organisations should run for cover after a breach. Even if you're not the direct cause, finger pointing and blame shifting are not winning strategies."

"Our sense is that a culture of denial still persists, particularly where a major breach hasn't yet occurred. Every new poorly-handled breach inflames end user demands for greater accountability and more laws. But we shouldn't have to have to wait for laws to dictate our trust processes. Businesses who rely on the internet have a collective interest in moving to best practice. Trust is fragile and ephemeral — it shouldn't be taken for granted," Coroneos said.

Of the 14 cases assessed, the score spread was as follows

C (1 case)	C – (3 cases)	D (3 cases)	D – (3 cases)	Fail (4 cases)
7%	21%	21%	21%	28%

Co-author and brand management expert, Michael Parker explained: "It was our rising sense of dismay in seeing how badly large and well resourced companies were handling their stakeholder communication that prompted us to write the book. Our message to organisations is this: Move to a more transparent and honest posture. Cyber breaches are a fact of life, the quicker we can move entities to a state of readiness, the better they'll survive the court of popular opinion."

The authors concluded: "Most of the cases involved easily preventable breaches. Along with technology and training, you need a parallel investment in communication readiness. Our cases show it might save executive careers."

Ends.

Details of the work and the authors > cyberbreachplaybook.com

Further comment: **Peter Coroneos** 0419 552 872   **Michael Parker** 0423 121 354

More:

Peter Coroneos led the Internet Industry Association from 1997-2011 and is now Regional Head Asia Pacific for the global NGO, Cybersecurity Advisors Network (CyAN).

Michael Parker is a noted brand-management and communication expert, and is MD of Praxis Communication, Sydney.

About the book's breach analysis:

Ten 'grade criteria' were used to assess the highly publicised breaches from 2015 to July 2018, including: the scale of the breach, the sensitivity of the information compromised, the time taken to report the breach, any evidence of a coverup, the time taken for management acceptance of responsibility, how predictable and preventable the breach was, the degree of public backlash and, where appropriate, notice and redress for affected individuals."

The breach cases reviewed were:

- Australian Bureau of Statistics - 2016 online census
- Australian Electoral Commission - 2016 election electronic voting security flaws
- Geoscience Australia July 2018 - national audit office report
- PageUp - 2018 job applicants data breached
- Uber 2017; 57 million records including 1 million Australian passengers and drivers
- Republican National Convention 2017 - 198 million voter records exposed by cloud error
- Equifax 2017, 143 million personal records stolen
- JP Morgan and Chase 7 million customer records exposed
- TalkTalk 2015 - UK telco 150,000 customer records breached
- Ticketmaster - 2018 breach exposing financial details
- Target - supply chain breach of its point of sale systems
- Verizon 2017 - 14 million customer records exposed
- Yahoo - largest ever reported data breach
- Ashley Madison - the infamous 2015 dating site hack