

Beyond the Breach: Uncovering the Untold Lessons from Australia's Cyber Crises.

A look back at cyber crisis and strategy failures and how to avoid them

John Karabin



Jesse Pearce



McGrathNicol
Advisory

“No plan survives first contact with the enemy”



Helmuth von Moltke ("The Elder"),
Prussian Field Marshal and renowned military strategist
1800-1891

“Everyone has a plan ‘till they get punched in the mouth”



[This Photo](#)

[CC BY-NC](#)

Mike Tyson, World Champion Heavy Weight Boxer
- 1987

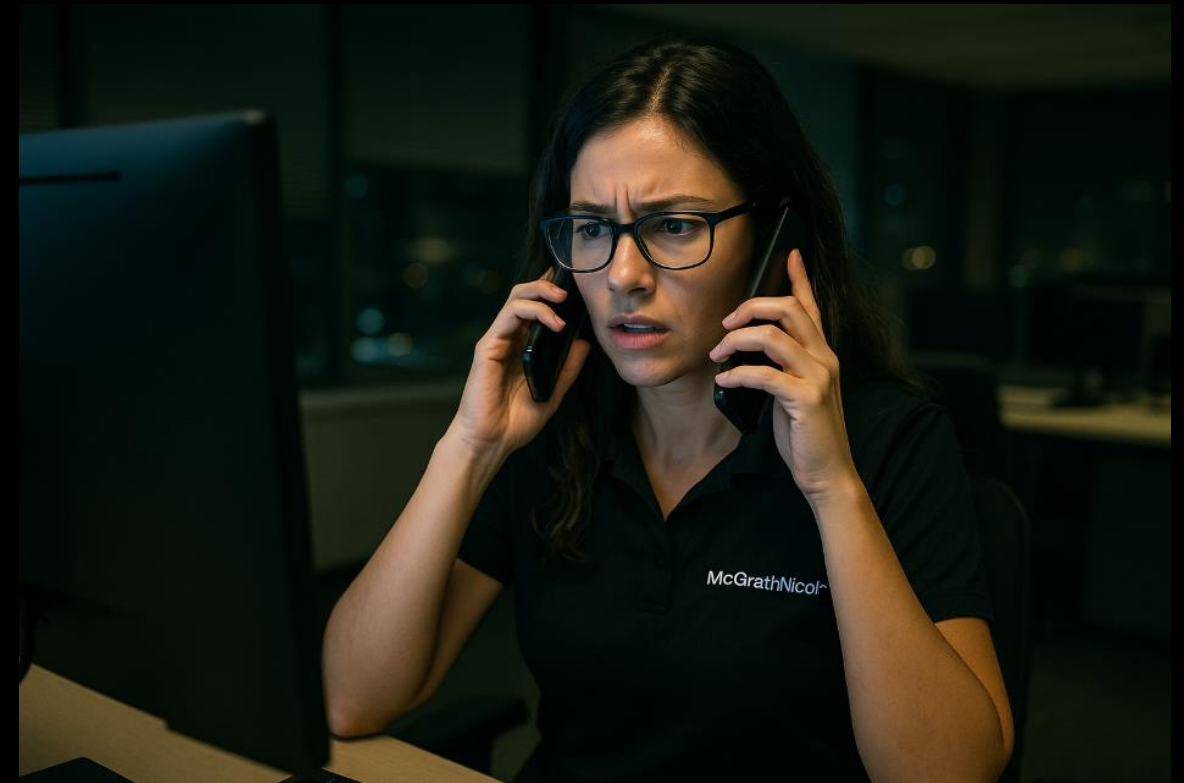
“ Over the next five years, a complex, challenging and changing security environment will become more dynamic, more diverse and more degraded.” – Mike Burges ASIO

- Scamwatch, ReportCyber, the Australian Financial Crimes Exchange (AFCX), IDCARE , ASIC state \$2.03 billion lost in 2024
- 110% increase in Ransomware – Zcaler 2025 Report
- Government has continued it's focus on setting cyber as a nationally strategic issue



70% of cases – 19.00 Friday evening before a long weekend. The phone's ring

"Hi McGrathNicol, something dreadful has happened...."



28% of cases – Ransomware



WARNING!

Your personal files are encrypted!

11:58:26

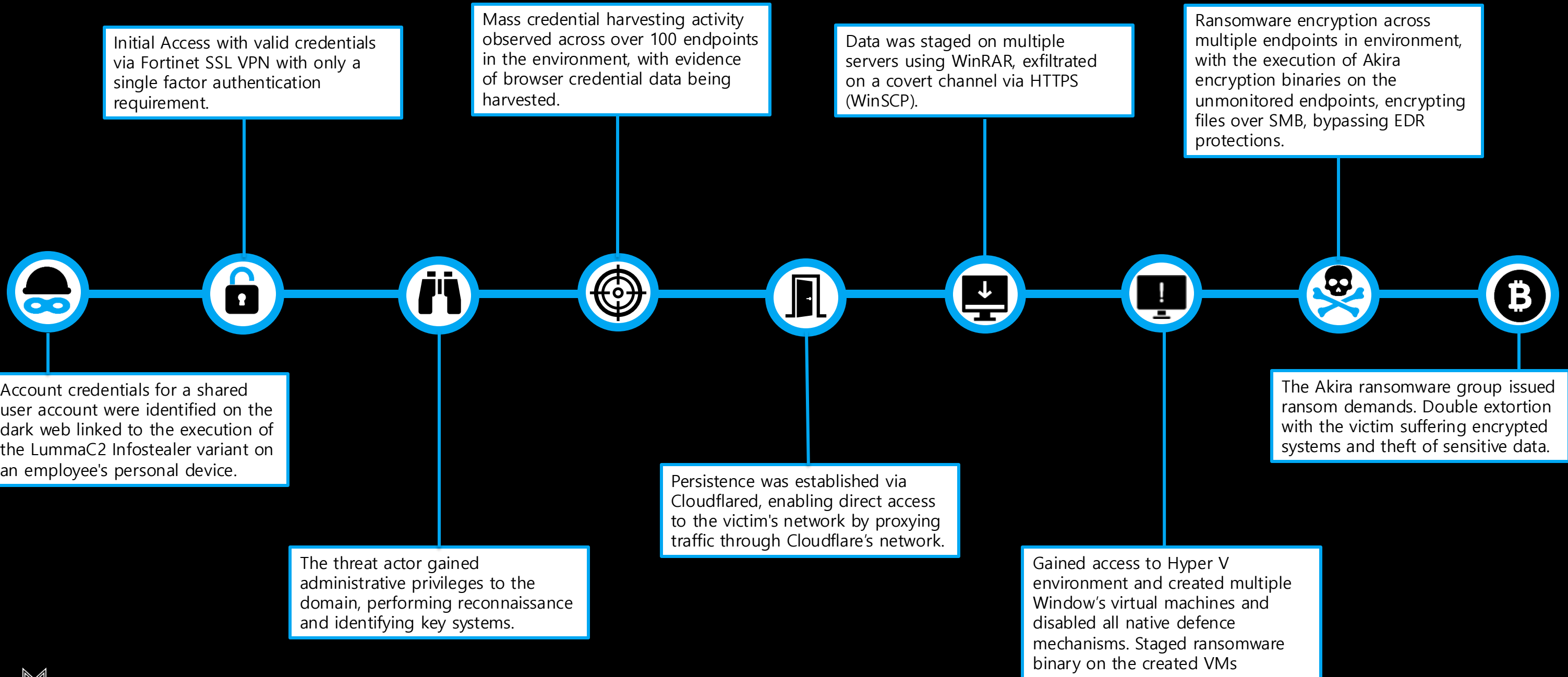
Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key. The server will eliminate the key after a time period specified in this window.

Open <http://maktubuyatq4rfyo.onion.link>
or <http://maktubuyatq4rfyo.torstorm.org>
or <http://maktubuyatq4rfyo.tor2web.org>

Case Study

McGrathNicol was engaged by an organisation targeted by the Akira ransomware group.

AKIRA



2% of cases – Major cyber events

- Misstep 1: Delayed detection / no detection
- Misstep 2: Poor internal / external communication
- Misstep 3: Lack of tested response plan
- Misstep 4: Failures in DR/BCP
- Misstep 5: Not considering the full impact of related systems and processes



Lessons Learnt from Flight QF32 – Crisis Management

- **Training for the Unexpected:** Prepare for multi-vector crises, not just isolated incidents. Prevent tunnel vision.
- **Resilience is Built Before a Crisis:** Invest in training, playbooks, gaming and simulations.
- **Crew Resource Management:** Enable cross-functional collaboration without silos prior to an event. RACI's and an Incident Controller (IC) are vital!
- **Trust & Teamwork:** Build trusted relationships before the breach. Know everyone!
- **Clear Communication:** Communicate with honesty and transparency to build trust.



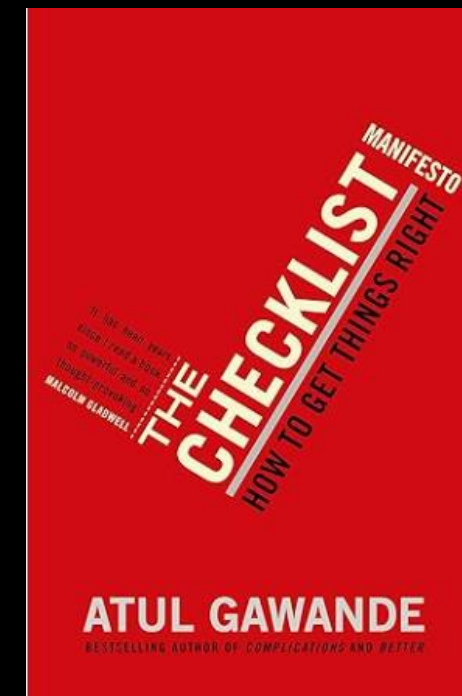
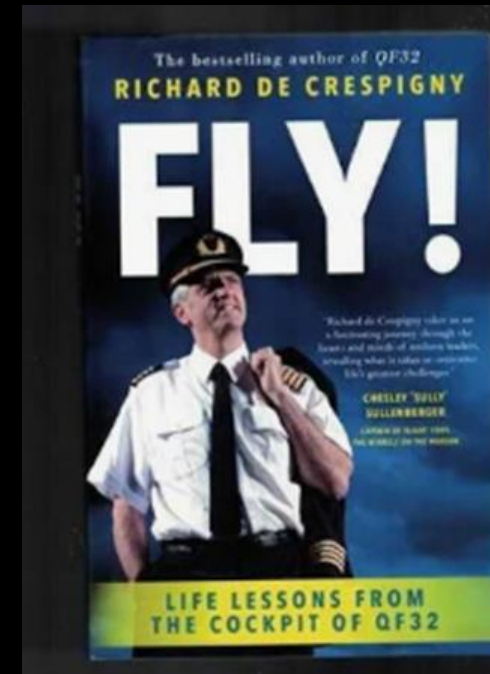
(Reuters)

Lessons Learnt from Flight QF32 – Crisis Management

- **Frameworks and Checklists:** CMP, IRP's, DR/BCP are vital, but don't over complicate and use playbooks as guides. Build in improvisation and adaptability as needed.
- Eg ANC, NITS, SITRep, ITASC, ARSO, DRSABCD

- **Growth from Adversity:** Use each breach as a free audit to improve defenses. Learn from Post Incident Reviews (PIR's) or After Action Reviews (AAR)

- **Leadership Under Pressure:** Project calm confidence and focus on priorities.



Thank you

John Karabin

<https://www.linkedin.com/in/johnkarabin/>

Jesse Pearce

<https://www.linkedin.com/in/jesse-pearce-69b4a2140/>

