PCI Security Standards Council

Reducing the Impacts of a Data Breach in the Not-For-Profit Sector

An industry that relies on Trust

PCI Security Standards Council

Stuart Campbell

Head of Customer Success, QuasarScan

QuasarScan

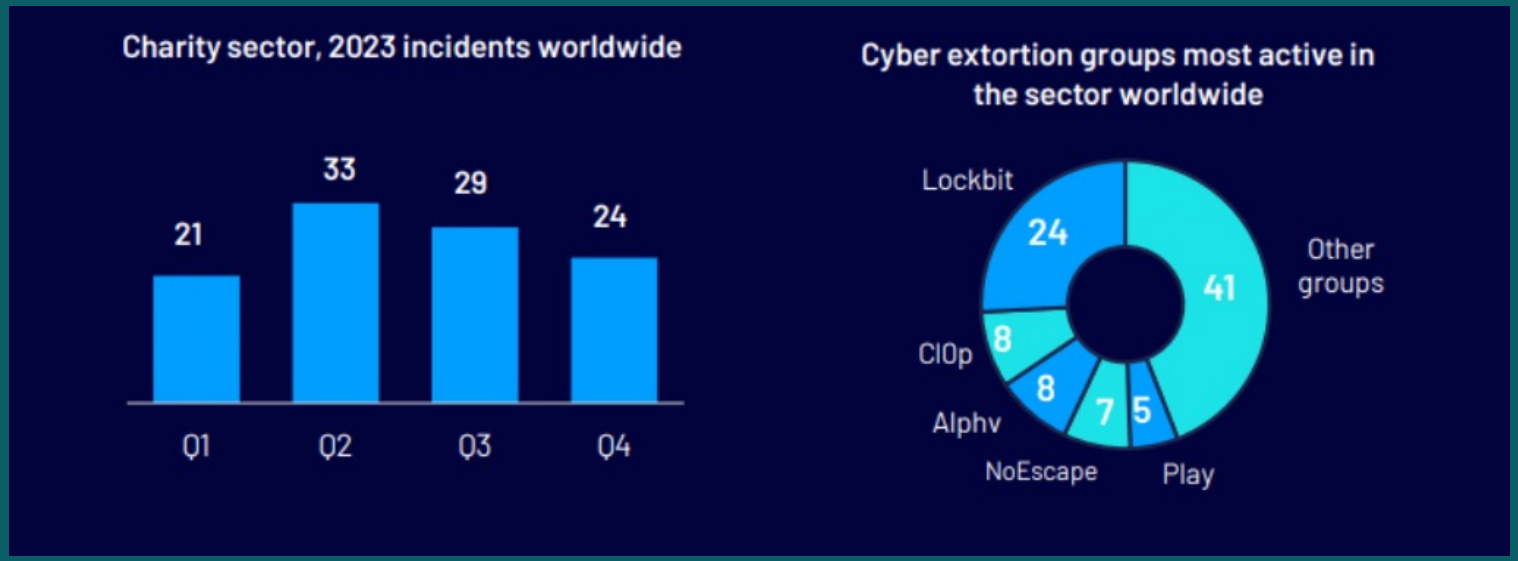
The Not-For-Profit (NFP) Sector Today

- A diverse range of organisations
  - Charities come in all different shapes and sizes, each with an extraordinary mission.
  - Globally, in 2023, the sector's market size topped $289b USD.
  - Organisations rely on the goodwill and trust of volunteers, supporters and donors to function.
- Some consistent challenges remain:
  1. Budget Constraints.
  2. Technology constraints.
  3. Heavy reliance on Third Party Service Providers (TPSP's).
  4. High dependency on donor trust.
  5. Commonly viewed as low-hanging fruit.

PCI Security Standards Council®

https://www.maximizemarketresearch.com/market-report/nonprofit-organizations-market/134550/

Notable Insights

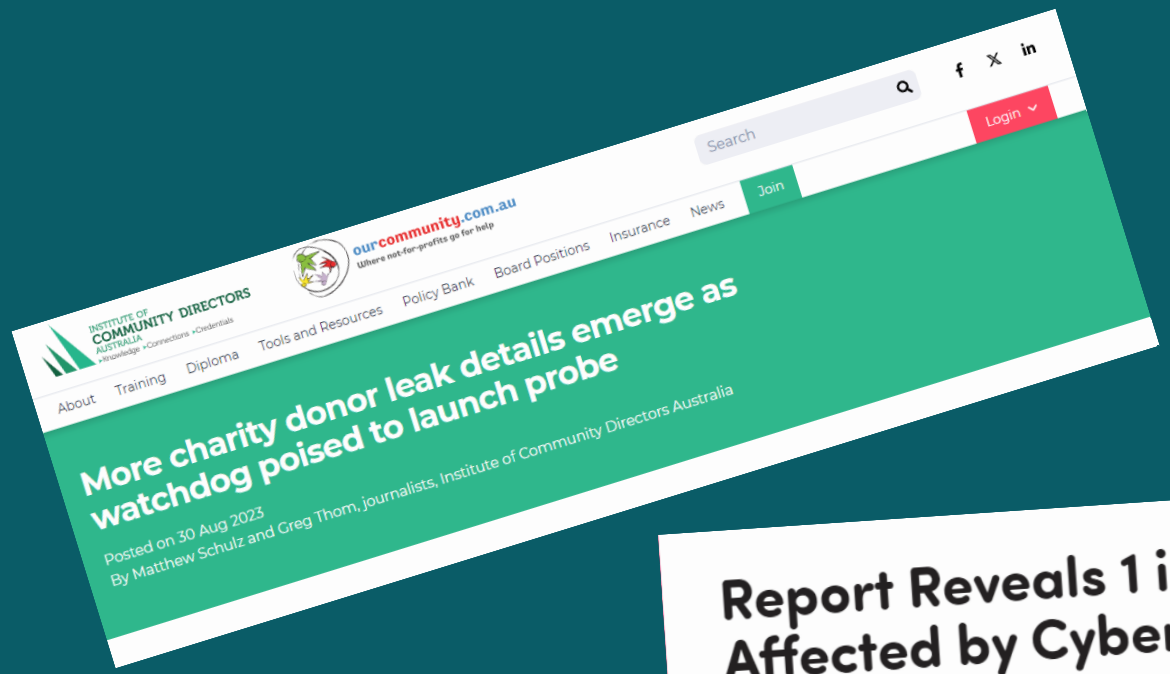


- In my own backyard (ANZ):
  - Only 43% of NFPs invested in cyber security in the last two years to 2022.
  - 37% of NFPs do not have effective procedures to detect and report data breaches.
  - One in five Australian charities and not-for-profits fears that a cyber security attack would devastate their organisation.

https://www.communitydirectors.com.au/articles/charities-in-fear-of-cybercrime-report
https://cybercx.com.au/resource/australian-charities-intelligence-insights/
https://www.grantthornton.co.nz/insights/cybersecurity-a-vulnerable-spot-for-nfps/

PCI Security Standards Council

When Things Have Gone Wrong…



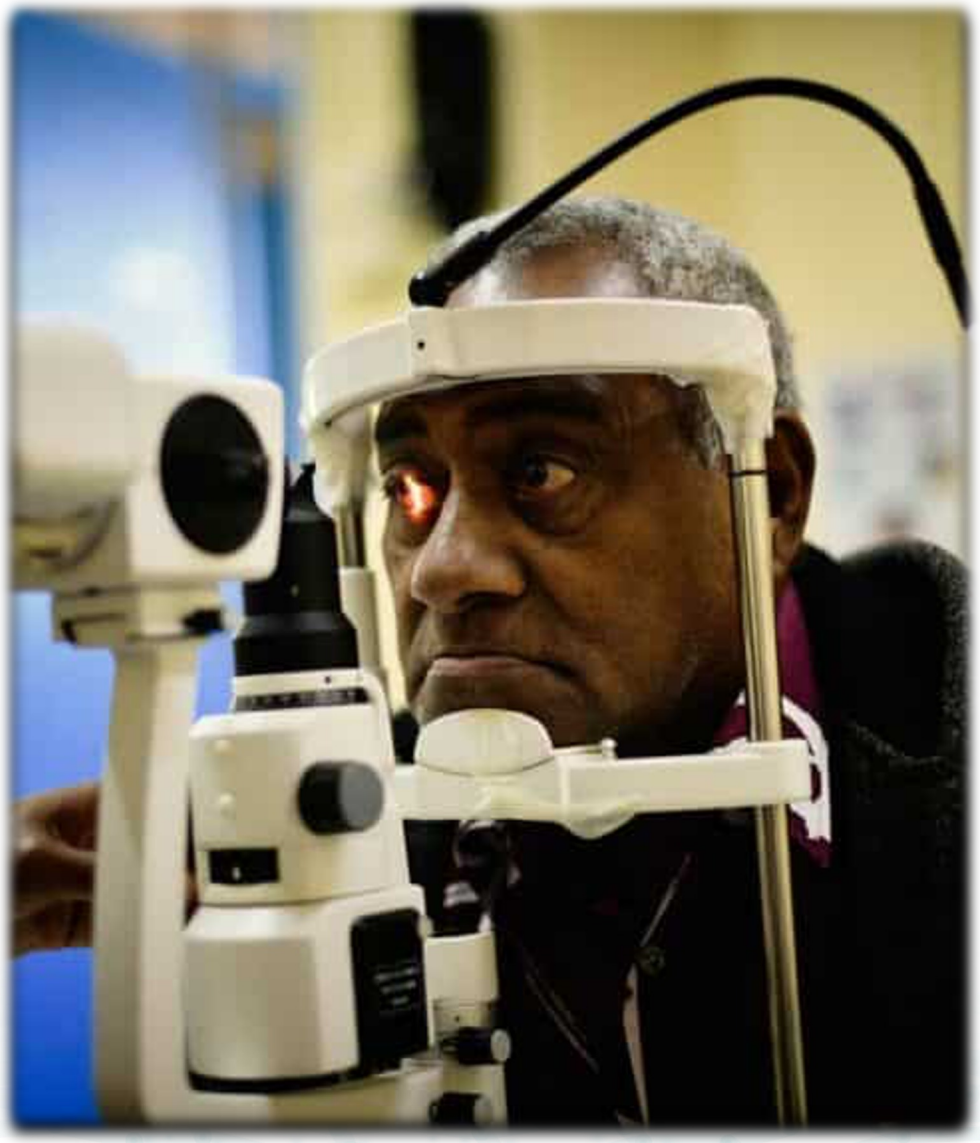
https://www.communitydirectors.com.au/articles/charity-donor-details-released-in-major-cyber-breach
https://www.infoxchange.org/nz/news/2023/04/report-reveals-1-6-asia-pacific-ngos-affected-cyberattack-past-12-months

PCI Security Standards Council

A Case Study

The Fred Hollows Foundation NZ

- A leading charitable organisation whose purpose is to **end avoidable blindness and vision impairment in the Pacific.**
- The Foundation relies on donations from various individuals, groups, and organisations to conduct their essential work.



The **Fred Hollows** Foundation NZ

PCI Security Standards Council

The Important Work of the Foundation

The gift of sight for Poufia

https://www.hollows.org.nz/longform/poufia

The Important Work continued…

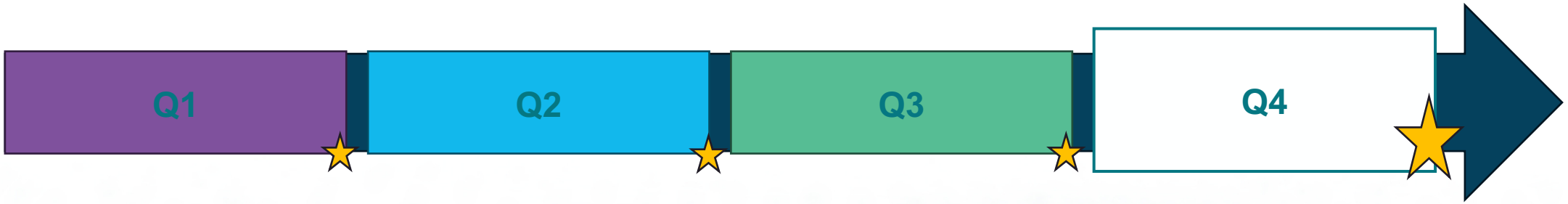
PCI Security Standards Council

https://www.hollows.org.nz/longform/poufia

Securing This important work

Ongoing assurance, proactive compliance

- In 2018, The Foundation embarked on a cyber uplift programme, which developed a mature and highly effective way to manage PCI DSS compliance.
  - Activities were treated as a **critical part of BAU.**
  - Any potential vulnerabilities are identified and addressed **early.** At the root cause.
  - Staff, service providers, and wider stakeholders were brought along the journey and shifted in mindset, which was driven directly by the Exec Team.



PCI Security Standards Council

Some Observations

How did the Foundation reduce the risk and likelihood of an Account Data Compromise?

1. Got the **buy-in and the remit.**

2. Reduced the impact by **removing unencrypted data.**

3. We reduced the likelihood of reoccurring by addressing the **root cause** and through a **proactive security programme.**

“When we commenced our PCI DSS compliance journey, it was like trying to complete a jigsaw without knowing you’re missing a few pieces! Our partners helped locate those missing pieces and initiate what has become a very successful and seamless programme which ensures we safeguard very sensitive data and maintain the trust of our valued donors.

In addition to meeting our PCI DSS compliance requirements, we significantly strengthened our overall cyber security position to what is now regarded as one of the best in class”

Sharon Orr, Chief Operating Officer, The Fred Hollows Foundation NZ

PCI Security Standards Council®

Key Takeaways

1. **Know your risk.** Understand what it represents, before addressing it in a way that is **enduring**.
2. Treat compliance as an **operational capability**, not a point-in-time requirement.
3. **Know your ecosystem.** Work with donors, sponsors, staff, service providers and the wider community.
4. **Market it.** Include your security and compliance progress, investment and development in industry papers, annual reports and to the wider industry.

PCI Security Standards Council®

The Important Work Continues

PCI Security Standards Council

Thank you

If you have any questions, come and find me!


PCi
Security
Standards Council
®