Institute of Community Directors Australia
(ICDA) NFP Governance Survey 2019

ICDA Spotlight Report:
Fraud & Cybercrime

September 2, 2019

Key Findings

Up to **one in five** not-for-profit organisations has **experienced some sort of crime relatively recently** (and some organisations experienced multiple crimes).

Theft of assets, cyber-hacking, credit card fraud and **theft of cash** are the **most commonly reported** crimes.

Around **two-thirds** of the crimes experienced by not-for-profit organisations are **not being reported to the police.**

Theft of cash and **theft of assets** are **more likely to be reported** to the police than other types of crime.

About The Survey

The Institute of Community Directors Australia (ICDA) surveyed 1878 senior leaders in the community sector in the six weeks leading to March 26, 2019.

Respondents came from all states and territories in Australia (with Victoria, New South Wales, Queensland and Western Australia dominating the sample), and were roughly evenly spread between the roles of senior management/CEO and board members.

Most respondents were involved in organisations in the community development; human services; education; health; arts and culture; and sports and recreation segments of the community sector.

The majority of respondents identified as women (71%), with 28% identifying as male and 0.48% non-binary.

This *ICDA Spotlight Report* presents a snapshot of results relating to how boards review their own performance and that of their organisation's head person (CEO, executive director, etc).

Further aspects of the survey will be released progressively over the next few months, with a final report incorporating all results to be released later in the year.

Detailed Results

A total of 19% of respondents said their organisation had experienced some type of crime in the 12 months prior to the survey.
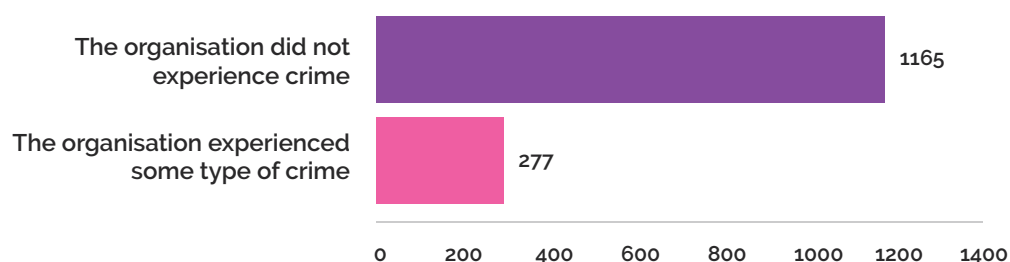
Fewer than 3% of respondents said they'd experienced cheque fraud, payroll fraud, bribery and kickbacks, theft of data, data ransom and/or expense-account fraud.

The areas of most concern, with the results reflecting some organisations reported more than one crime, were:

· **Theft of assets** (reported by 7% of survey respondents);
· **Cyber-hacking** (7%);
· **Credit card fraud** (4%); and
· **Theft of cash** (3%).

Crime

Number of ICDA survey respondents who said that in the previous 12 months...

The organisation did not experience crime	1165
The organisation experienced some type of crime	277

(Chart x-axis: 0, 200, 400, 600, 800, 1000, 1200, 1400)

Note: the figures shown above include all survey respondents who responded to this question. A total of 23% of survey participants opted not to respond to this question.

Important notes:

Our survey did not identify individuals nor individual organisations. As such, it is not possible to say how many cases of crime may have been reported by multiple people from the same organisation and thus effectively double-counted in our survey analysis. It is expected, however, that any rate of overcounting would be equalled by under-reporting.

Note too that due to the relatively small number of organisations that indicated they had experienced a crime, we were unable to explore sector or organisation size-based differences (with just 277 organisations reporting some sort of crime, the sample was too small to allow us to split the data further).
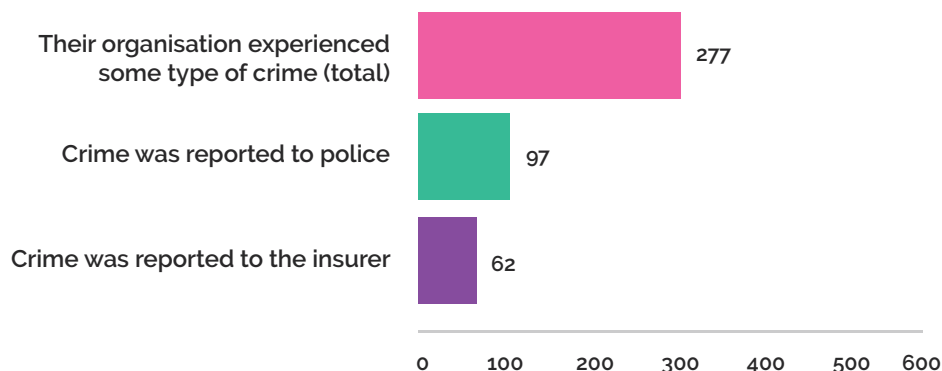
Many crimes are going unreported. Just one in three of the respondents who said their organisation had experienced crime in the previous 12 months said that the case was reported to the police. Even fewer (just one in five) was reported to insurers.

Out of those who said their organisation had experienced some kind of crime (277, or 19% of all survey responses):

• 35% said the incident was reported to the police
• 22% said the incident was reported to their insurer.

Crime

Number of ICDA survey respondents who said that in the previous 12 months...

Their organisation experienced some type of crime (total)	277
Crime was reported to police	97
Crime was reported to the insurer	62

(Chart x-axis: 0, 100, 200, 300, 400, 500, 600)

We found some evidence to suggest that some organisations had experienced more than one type of crime in the year leading up to the survey.

For example:

- **20%** of those who said they had experienced theft of assets (20 respondents) also said they'd experienced theft of cash, and **15%** (14 respondents) also experienced expense-account fraud
- **12%** of those who said they had experienced cyber-hacking (11 respondents) also mentioned credit card fraud.

It is not known if any of the multiple crimes reported by any one respondent resulted from a single incident.

Breakout of crime cases:

THEFT OF ASSETS:

A total of 96 respondents (7% of the sample) said their organisation had experienced theft of assets in the previous 12 months. Of those:

38%
did not know who the perpetrator was

16%
said the perpetrator was a **staff member**

10%
said the perpetrator was a **volunteer**

5%
said the perpetrator was an **online fraudster**

"Other" perpetrators (identified by **18%** of respondents) included **non-associated members** of the public/community, **strangers** who broke into a facility, or **users** of the service.

A total of 49% of those who had experienced theft of assets said the case was reported to the police and 28% said the case was reported to their insurer.
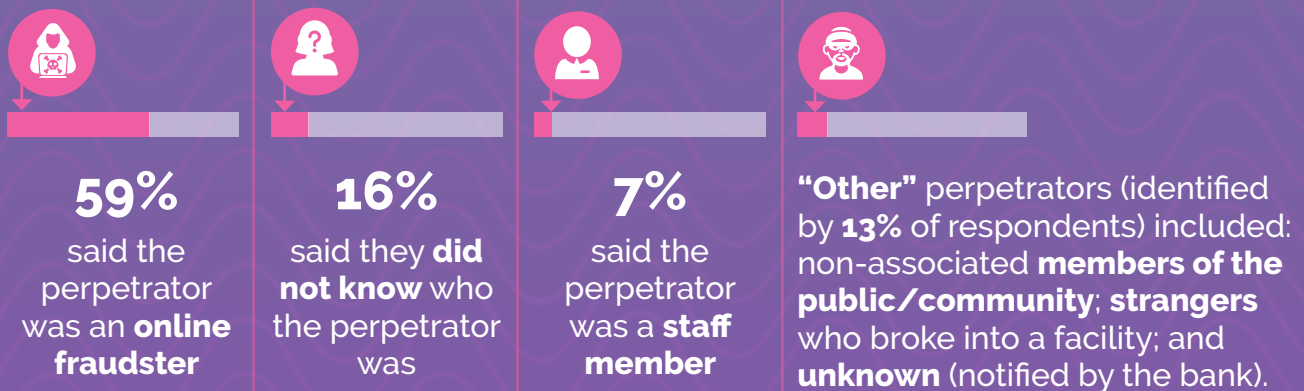
CYBER-HACKING:

A total of 94 respondents (7% of the sample) said their organisation had been cyber-hacked. Of those:

53%
said the perpetrator was an **online fraudster**

31%
said they **did not know** who the perpetrator was

5%
said the perpetrator was a **staff member**

A total 27% of those who had experienced cyber-hacking said the case was reported to the police and 23% said that the case was reported to their insurer.
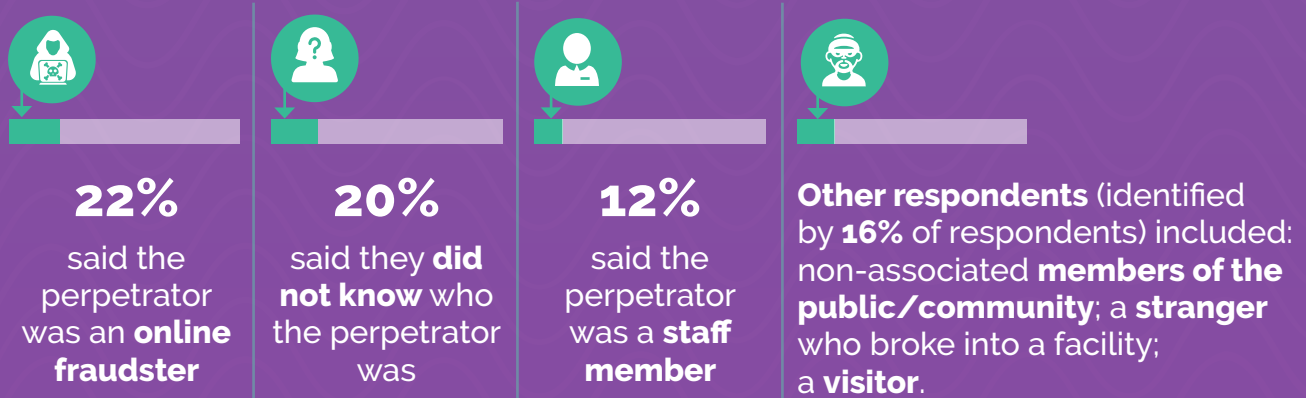
CREDIT CARD FRAUD:

A total of 56 respondents (4% of the sample) said their organisation had experienced credit card fraud. Of those:

59%
said the perpetrator was an **online fraudster**

16%
said they **did not know** who the perpetrator was

7%
said the perpetrator was a **staff member**

"Other" perpetrators (identified by **13%** of respondents) included: non-associated **members of the public/community**; **strangers** who broke into a facility; and **unknown** (notified by the bank).

A total of 29% of those who had experienced credit card fraud said the case was reported to the police and 16% said the case was reported to their insurer.

THEFT OF CASH:

A total of 49 respondents (3% of the sample) said their organisation had experienced theft of cash. Of those:

22%
said the perpetrator was an **online fraudster**

20%
said they **did not know** who the perpetrator was

12%
said the perpetrator was a **staff member**

Other respondents (identified by **16%** of respondents) included: non-associated **members of the public/community**; a **stranger** who broke into a facility; a **visitor**.

A total of 41% of those who had experienced theft of cash said the case was reported to the police and 24% said the case was reported to their insurer.

Other crime characteristics of note

Detailed analysis of the survey results indicate that:

- Most cases of credit card fraud (at least 59%) and cyber-hacking (at least 53%) are perpetrated by online fraudsters.
- The crimes of 'theft of cash' and 'theft of assets' are more likely to be reported to the police than other types of crime – around half of these incidents were reported to the police.
- Credit card fraud is less likely than other types of crime to be reported to insurers. Only 16% of cases were reported to insurers, compared with more than 24% in the other types of frauds/crimes. This is most likely because credit card frauds are often identified and protected by the bank who issued the card (as pointed out by several respondents).
- It is difficult to identify the perpetrator of theft of assets. For around 40% of the cases the respondent did not know who the perpetrator was.

Feedback/Recommendations/Next Steps

What do you make of these results? How should the sector, and those who work to resource and upskill the sector, respond?

Send your feedback to service@ourcommunity.com.au, tweet us at @OurCommunityAU, tag us on Facebook at @OurCommunity.com.au, and contribute to the conversation in our Facebook group, Not-for-profit Happy Hour Australia.

We'll incorporate feedback into our final report, which is due for release later in the year.

If you would like to be notified when further ICDA Spotlight Reports are released, join up as a member of the Institute of Community Directors Australia – visit www.icda.com.au to find out more.

About Institute of Community Directors Australia

The Institute of Community Directors Australia (ICDA) is Australia's best-practice governance network for not-for-profit boards, committees, councils, schools, and their staff.

An Our Community enterprise, ICDA delivers information, tools, training, events, qualifications and credentials to not-for-profits of all kinds. Activities include:

- Spearheading the Festival of Community Directors, a year-long program of events designed to celebrate and educate not-for-profit board members and the senior staff who support them

- Delivering Australia's premier nationally recognised qualification for not-for-profit leaders, the Diploma of Business (Governance) [in partnership with our partner Federation Training]

- Pioneering new governance training methods, including our landmark online compact courses

- Providing a suite of governance tools, including a range of practical helpsheets, templates and books, plus a free Board Matching Service and a free Policy Bank

- Face-to-face and online peer networking and support

- Regular newsletters to keep members informed and in touch

ICDA is led by the innovative members of the Our Community founding team, Denis Moriarty (Our Community Founder and Group Managing Director) and Patrick Moriarty (Institute of Community Directors Australia Executive Director), with input from the Our Community Board, comprising founding Chair Carol Schwartz and ethicist Dr Simon Longstaff.

Its work is guided by the Community Directors Council, which is chaired by Associate Professor Susan Pascoe AM, alongside 10 Australian community sector luminaries.

Find out more about ICDA at www.icda.com.au

**This report has been prepared for ICDA
by the Our Community Innovation Lab.**

**Visit:
www.ourcommunity.com.au/innovationlab**

Appendix: What questions are analysed in this report?

- **Qu 7: What is your organisation's approximate annual revenue?**
  [Less than $50,000; $50,001 - $250,000; $250,001 - $1 million; $1 million - $10 million;
  $10 million - $100 million; $100 million +; Don't know/would rather not say]

- **Qu 8: Select the one of the main field in which your organisation works**
  [Agriculture, fisheries and forestry; Animal welfare; Arts and culture; Community development;
  Economic development; Education; Environment; Health; Human rights; Human services (including
  disability organisations); Information and communications; International relations; Public affairs;
  Public safety; Religion; Science; Social sciences; Sport and recreation; Other – please specify]

- **Qu 26: Has your organisation experienced any of the following incidents in the past 12 months?**
  [Theft of cash; Theft of assets; Credit card fraud; Cheque fraud; Expense-account fraud; Payroll fraud;
  Bribery and kickbacks; Cyber-hacking; Theft of data; Data ransom; None of these]

- **Qu 27: Who was the perpetrator of the crime your organisation experienced? (if you have
  experienced more than one incident over the past 12 months, select the response that relates
  to the most significant incident)**
  [Not applicable; Staff member; Volunteer; Board member; Treasurer; Contractor; Another organisation;
  Online fraudster; Don't know; Other]

- **Qu 28: Was it reported to the police?**
  [Yes; No; Don't know/don't want to say]

- **Qu 29: Was it reported to your insurer?**
  [Yes; No; Don't know/don't want to say]