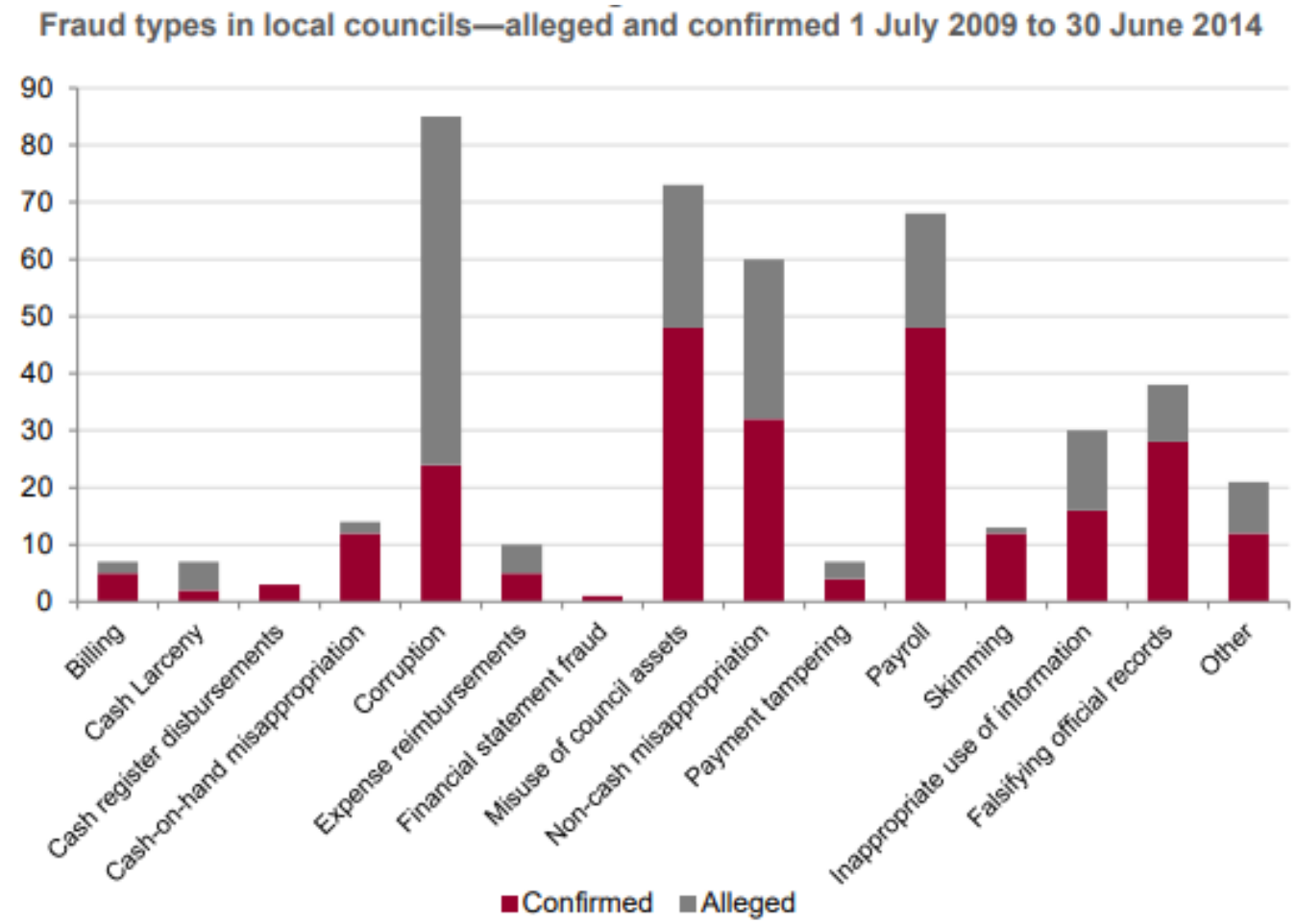
NOOSA'S FRAUD MITIGATION EXPERIENCE

Local Government Finance Professionals

CFO Conference 2019


FRAUD
FRAUD EVERYWHERE

Occurrence of Fraud in Local Government



Source: Queensland Audit Office from council survey

Some Key Trends…

$1 Billion Cost Nationally	• Direct cost to the Australian Economy from Cybercrime *(Cyber Security Review)*
67% Breached	• Share of Australian businesses subject to cyber security breach in 2018 *(Telstra Security Report 2019)*
17% Assess the Risk	• Only 11 of 66 reviewed QLD councils conduct fraud risk assessment every 2 years *(QAO Fraud in Local Govt Report 2016)*
15% Staff Trained	• Only 15% of NSW Councils provide training to their staff on fraud protection *(NSW LG Fraud Control Report 2018)*

Noosa's Experience – Ongoing Phishing and Malware Hits

- ICT controls detect and isolate around **3,000 email threats** per month (90% phish & 10% malware)
- **3 – 4 per month** make it through ICT security measures to the AP & Payroll Mailboxes
- No protection where the **supplier's email** has been compromised (example - office.com hacked)
- Ongoing hacking attempts to Council's system from international sources (international logins now blocked)

Biggest Risk for Noosa Council at Present

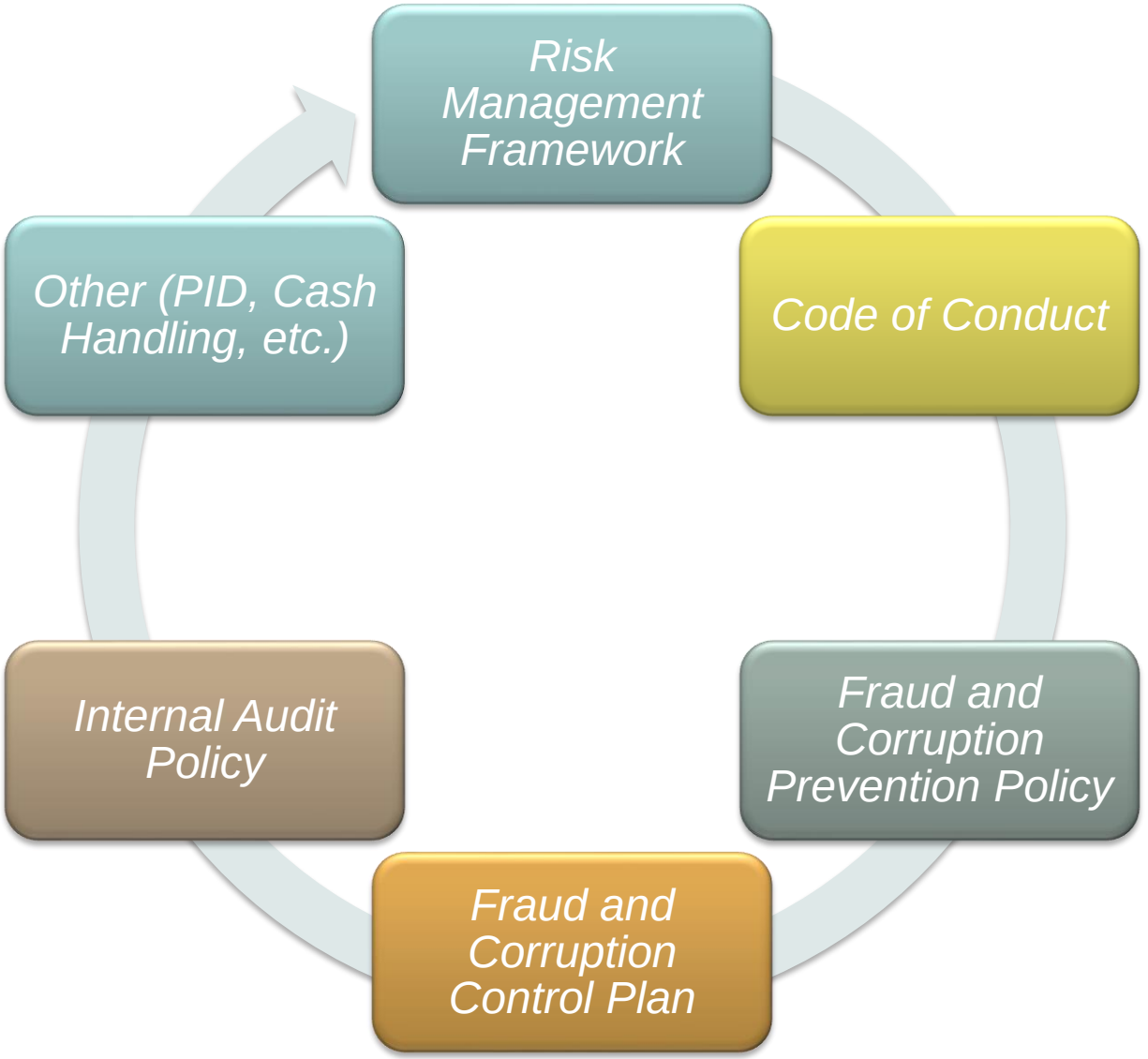
Manual steps in our processes not being followed…

(both in terms of input and validation checks)

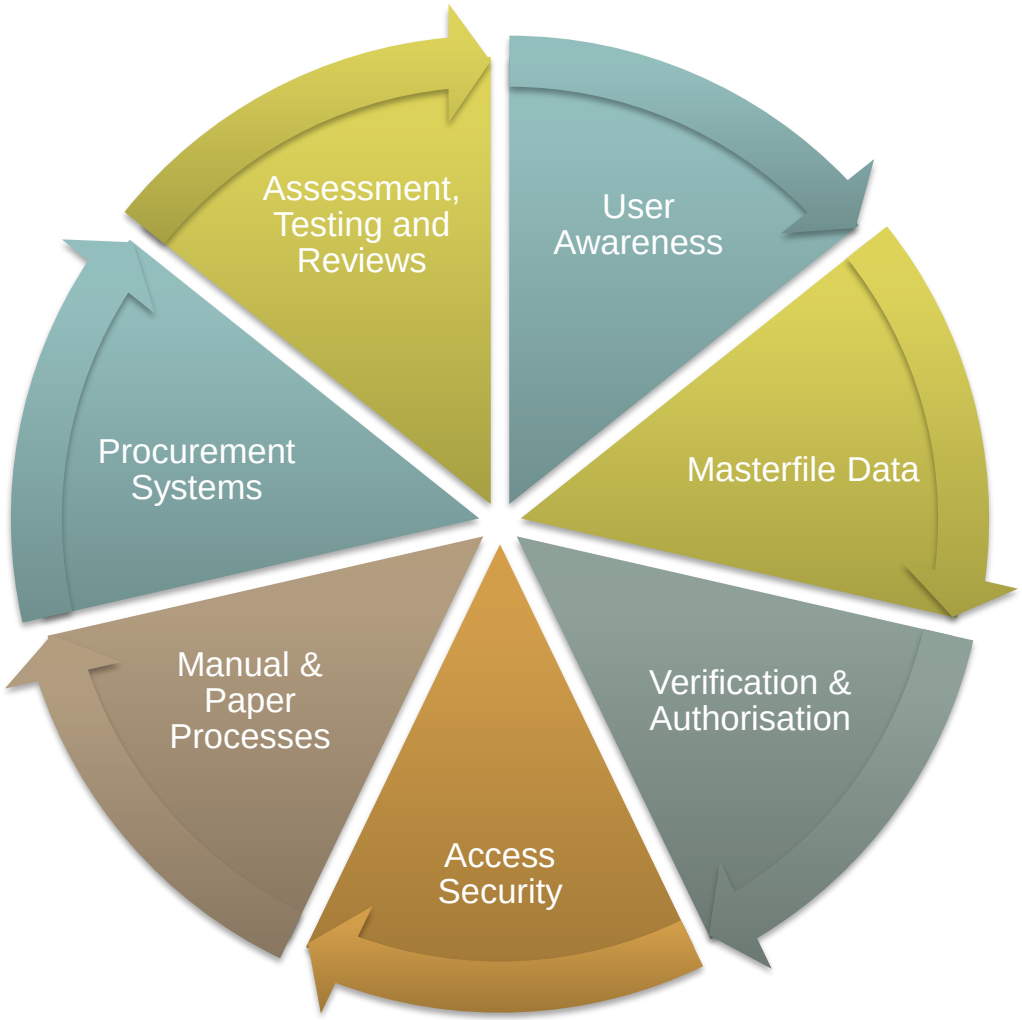
Best Practice Guidance

- Australia/New Zealand Standard AS/NZS ISO 31000:2009 - *Risk Management – Principles and Guidelines*
- Australian Standard, AS 8001-2008 – *Fraud and Corruption Control*
- Queensland Audit Office Report to Parliament 19: *2014-15 Fraud Risk Management in Local Government*
- Crime and Corruption Commission – *Fraud and Corruption Control Best Practice Guide 2018*
- Queensland Audit Office Report to Parliament 6: *2017-18 – Fraud Risk Management*

Noosa Council Framework



Current Target Areas for Noosa – Prevention Controls



User Awareness – Mandatory Online Training

Cyber-safety: Sextortion

Quiz

15 Jul 2019

Cyber-safety : Social Engineering

Quiz

01 Jul 2019

Cyber-safety: Ransomware

Quiz

31 May 2019

Cyber-safety: Impersonation

Quiz

29 Apr 2019

Cyber-safety: Introduction

Quiz

19 Mar 2019

Cyber-safety: Email Security

Quiz

19 Mar 2019

Cyber-safety: Passwords

Quiz

20 Feb 2019

User Awareness – Phishing Tests

Phishing Campaign

2019 July 16

Started: July 17, 2019
Ending: August 16, 2019

80%
292 Emails sent

24%
70 Emails opened

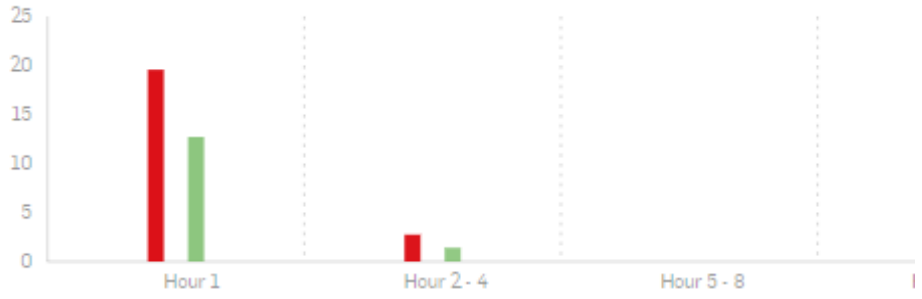
19 Re

Campaign response timeline

Fastest caught
[redacted]
38 seconds after receiving the email

Fastest reporter
[redacted]
51 seconds after receiving the email

13 sec — Time an attacker would have to operate before you were alerted.



Device breakdown

Type	Opened on	Caught on
Desktop	59% 41 of 70	92% 22 of 24
Mobile	19% 13 of 70	8% 2 of 24

User Behavior

Ideal behavior	5% reported the email without being caught
Good behavior	1% caught but reported the email
Neutral behavior	76% never opened the email
Not ideal behavior	10% opened the email but did not report it
Risky behavior	7% caught and did not report it

Masterfile Controls and Authorisation
(Following Internal Audit on Procure to Pay)

Current Steps

1. Not just bank acct details – consider contact details!
2. Supporting documentation
3. Phone verification using phone number from business website (not from the Masterfile contacts)
4. Manager review & signoff all changes each week

Future Improvements Planned

- System workflow approval for each Masterfile change
- ASIC search and verification (e.g. related parties)
- Pay ID
- Supplier Portal

(https://www.technologyonecorp.com/__data/assets/pdf_file/0016/100186/FACT18_Supplier_Portal_SCM.pdf)

Automating Manual & Paper Processes Where Possible

Underway

- Direct-to-bank payment processing to remove any user access to payfiles (T1 - Commbiz Automated)

- Online forms and business process automation
  - Online forms for staff on / off-boarding
  - Sundry Creditors

  (Automated Workflow approvals, enforced stage-gates, automation of system change processes)

Procurement Systems

Current Steps

- New procure-to-pay system implemented in June 2019
- No workarounds raising PO's if above ITQ threshold
- Standard system for all tender/quote evaluations
- Widespread use of Purchase Cards

Future Improvements Planned

- Review of sundry creditor process (Non-PO)
- Review of Purchase Card policy
- Merchant type restrictions on purchase cards
- Contracts register integrated to Procurement system
- Dashboard exception reporting (e.g. annual non-ITQ spend by supplier)

Access Security

Target

- Both Prevention and Detection
- Overall access breaches
- Changes to access and financial delegations
- Mitigating inherent access
- Higher risk – managers, finance, payroll, ICT, self approval purchasing officers

Constraints

- Significant amount of constantly moving data
- Multiple systems / modules
- Complexity of positions, roles & functions
- Resource impost
- Snapshot – Period A vs B
- Software upgrades and patches

End of Presentation