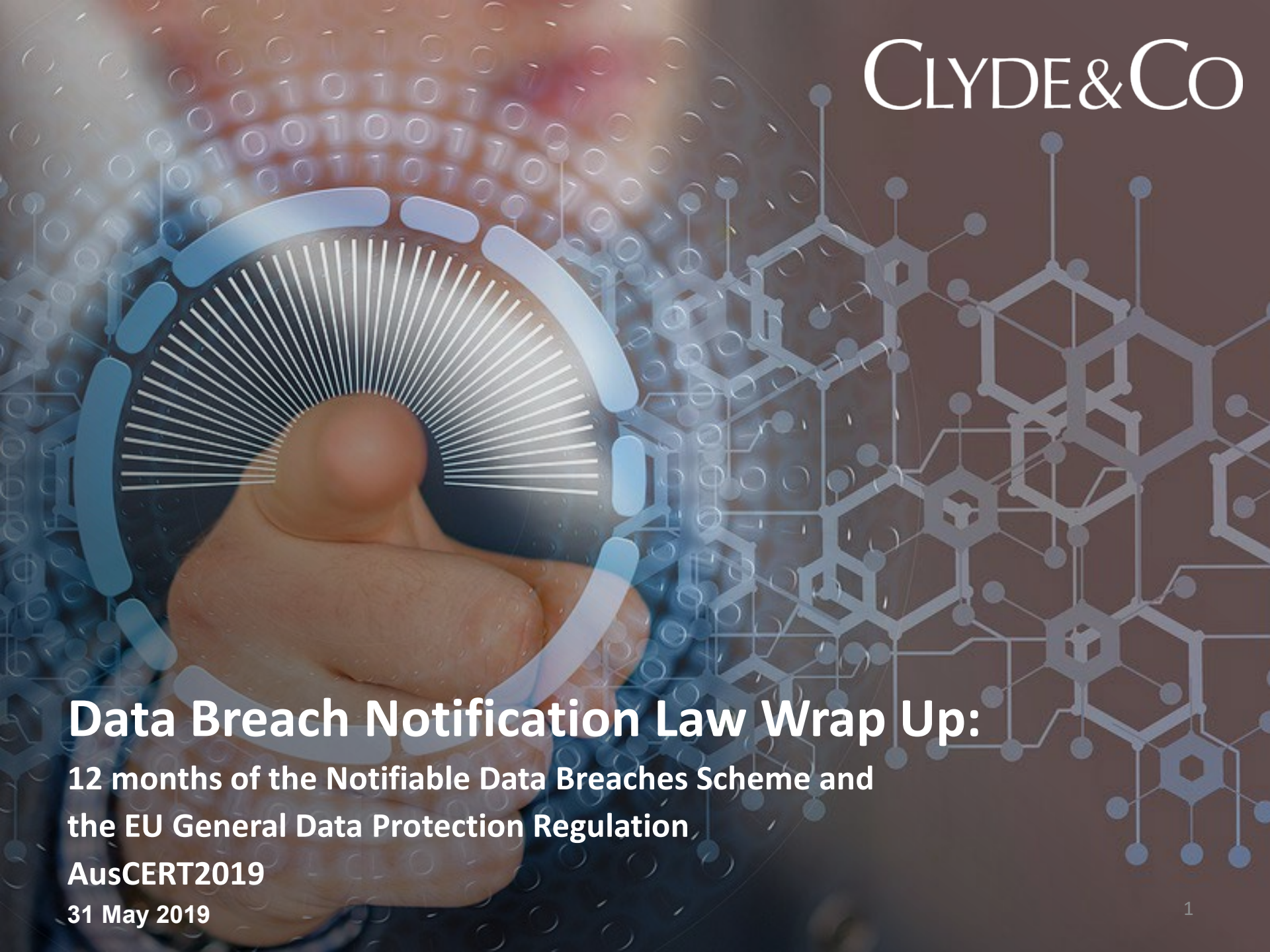


Data Breach Notification Law Wrap Up:

12 months of the Notifiable Data Breaches Scheme and the EU General Data Protection Regulation

AusCERT2019

31 May 2019

Overview of session

CLYDE&CO

We aim to cover…

- Australian regulatory landscape
- Key takeaways from the OAIC Notifiable Data Breaches Scheme 12 month report
- GDPR statistics, key trends and misconceptions
- Key trends arising from notifiable data breaches
- Common incident response issues and privacy implications arising in business email compromise and ransomware
- Future trends and issues

Notifiable Data Breaches Scheme

CLYDE&CO

APPLICABLE TO WHO?

APP entities subject to *Privacy Act 1988* (Cth)

WHAT TO INVESTIGATE

Suspected Eligible Data Breaches

1. Has there been a data breach?
2. Is serious harm likely?
3. Can remedial action be taken to prevent likely risk of serious harm?

WHEN TO NOTIFY?

As soon as practicable

WHO / HOW TO NOTIFY?

OAIC and affected individuals - by ordinary means

PENALTIES

Currently up to AUD 2.1 million civil penalty (organisations) but new amendments proposed

The regulatory landscape

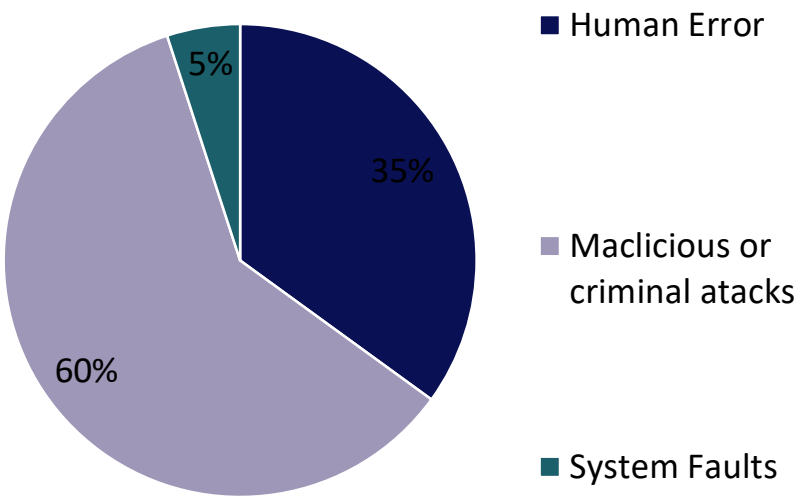
CLYDE&CO

Australian data breaches: 1 April 2018 to 31 March 2019

1,132 OAIC notifications comprising:

- 964 Eligible Data Breaches
- 186 Voluntary Notifications
- **712% increase** in data breach reporting

Causes of Data Breaches



Top 5 Industry Sectors

Health Services Providers	206
Finance	138
Legal, Accounting & Management Services	100
Education	75
Personal Services	36

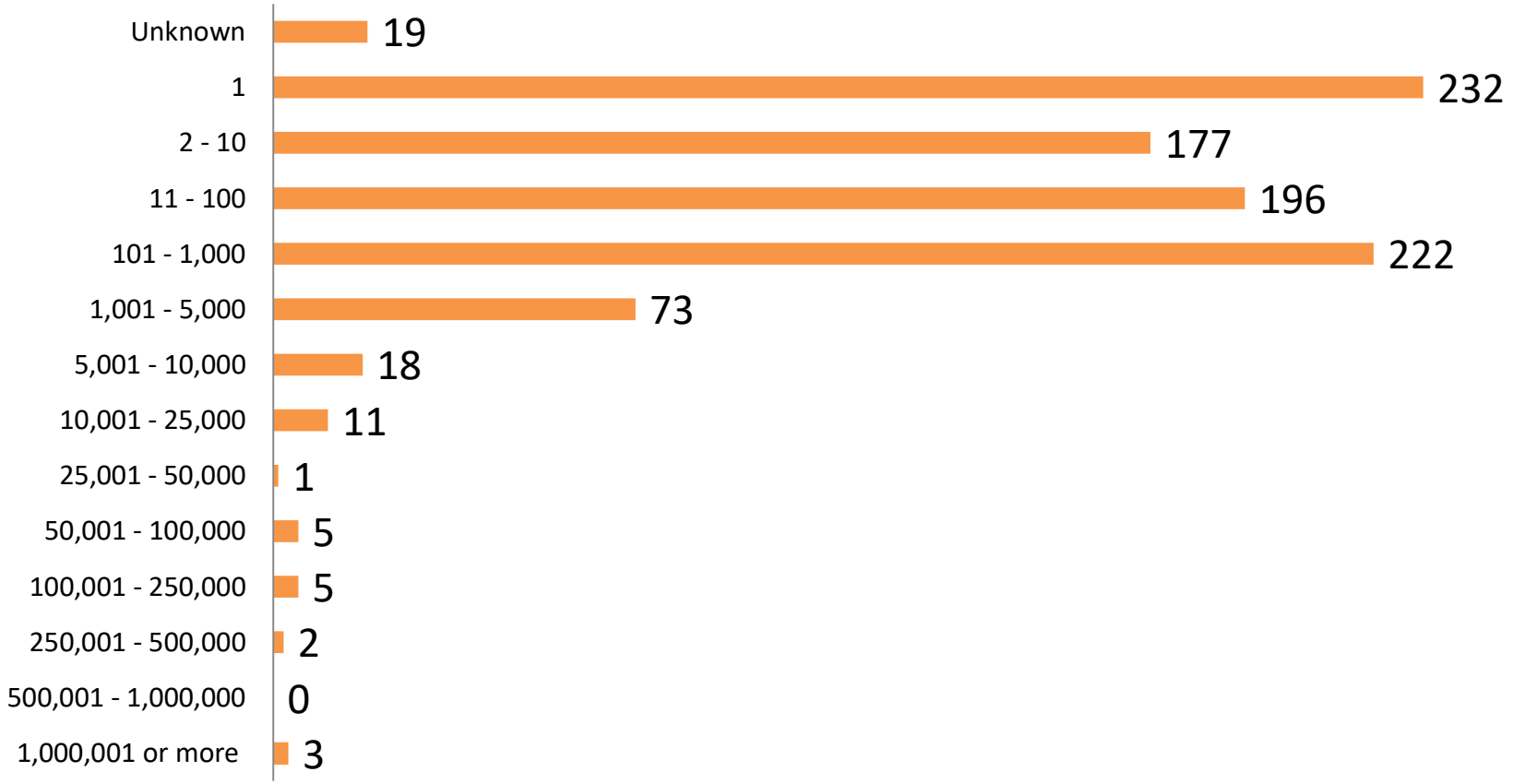
Source: Notifiable Data Breaches Scheme 12-month Insights Report, Office of the Australian Information Commissioner, 13 May 2019

The regulatory landscape

CLYDE&CO

Australian data breaches: 1 April 2018 to 31 March 2019

Number of individuals affected by breaches – all Sectors



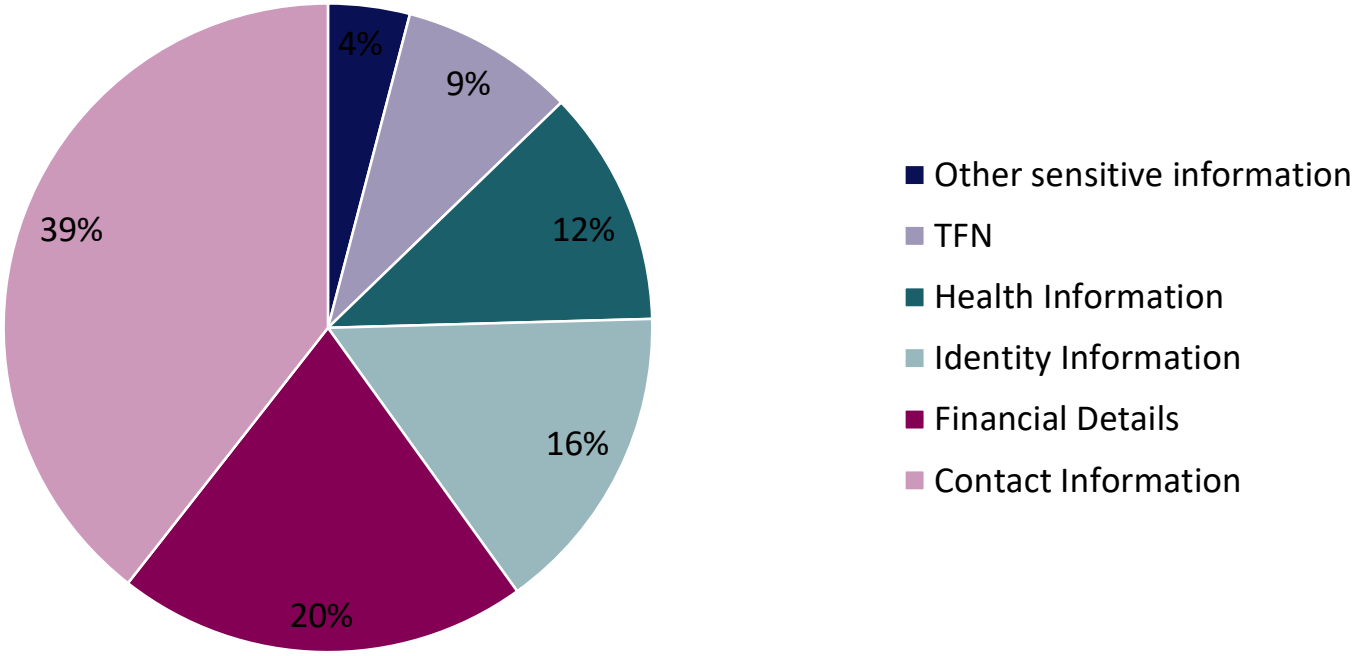
Source: Notifiable Data Breaches Scheme 12-month Insights Report, Office of the Australian Information Commissioner, 13 May 2019

The regulatory landscape

CLYDE&CO

Australian data breaches: 1 April 2018 to 31 March 2019

Types of Information involved in breaches:



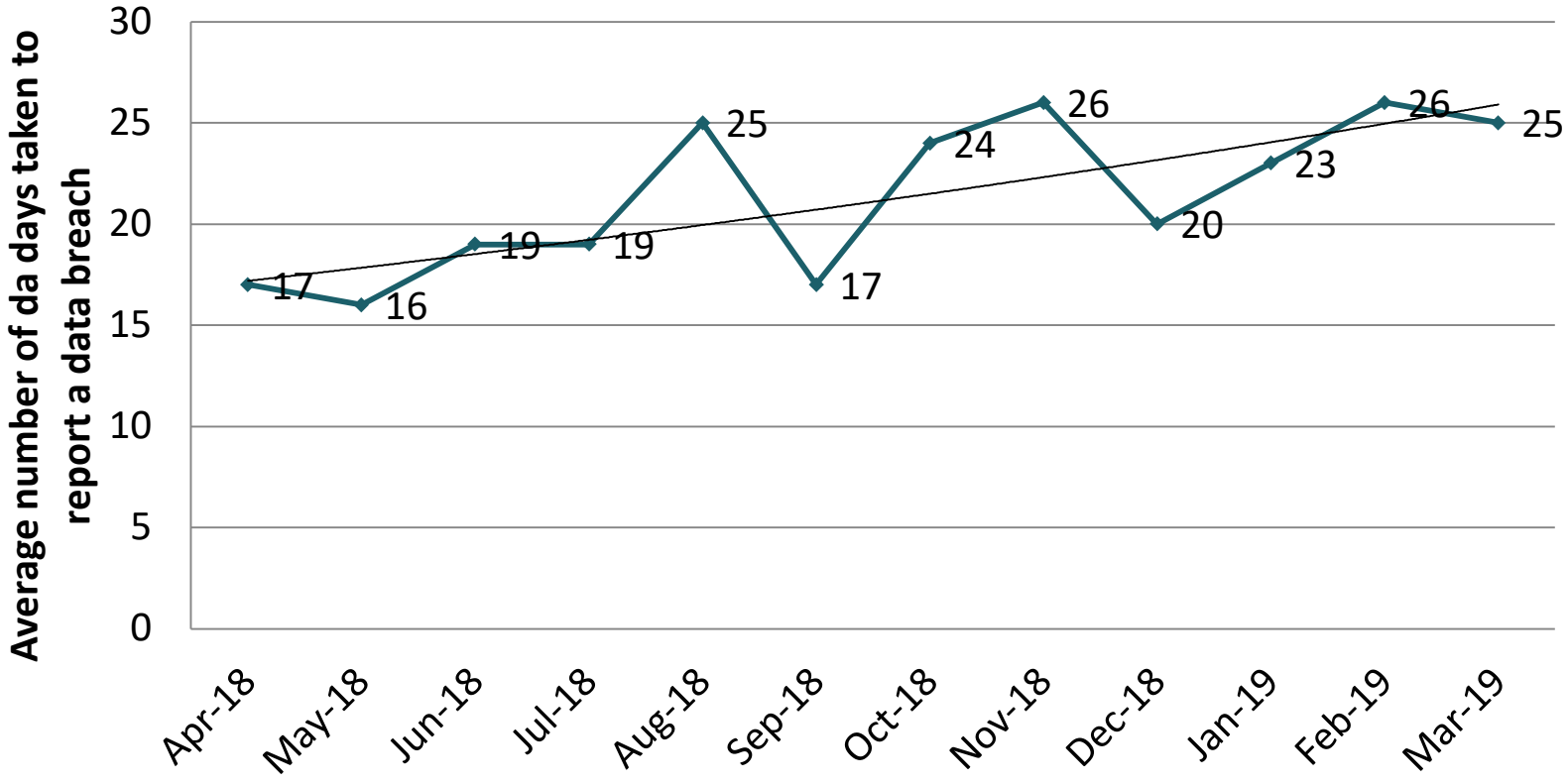
Source: Notifiable Data Breaches Scheme 12-month Insights Report, Office of the Australian Information Commissioner, 13 May 2019

The regulatory landscape

CLYDE&CO

Australian data breaches: 1 April 2018 to 31 March 2019

Average time to notify OAIC after becoming aware of the breach (in days)

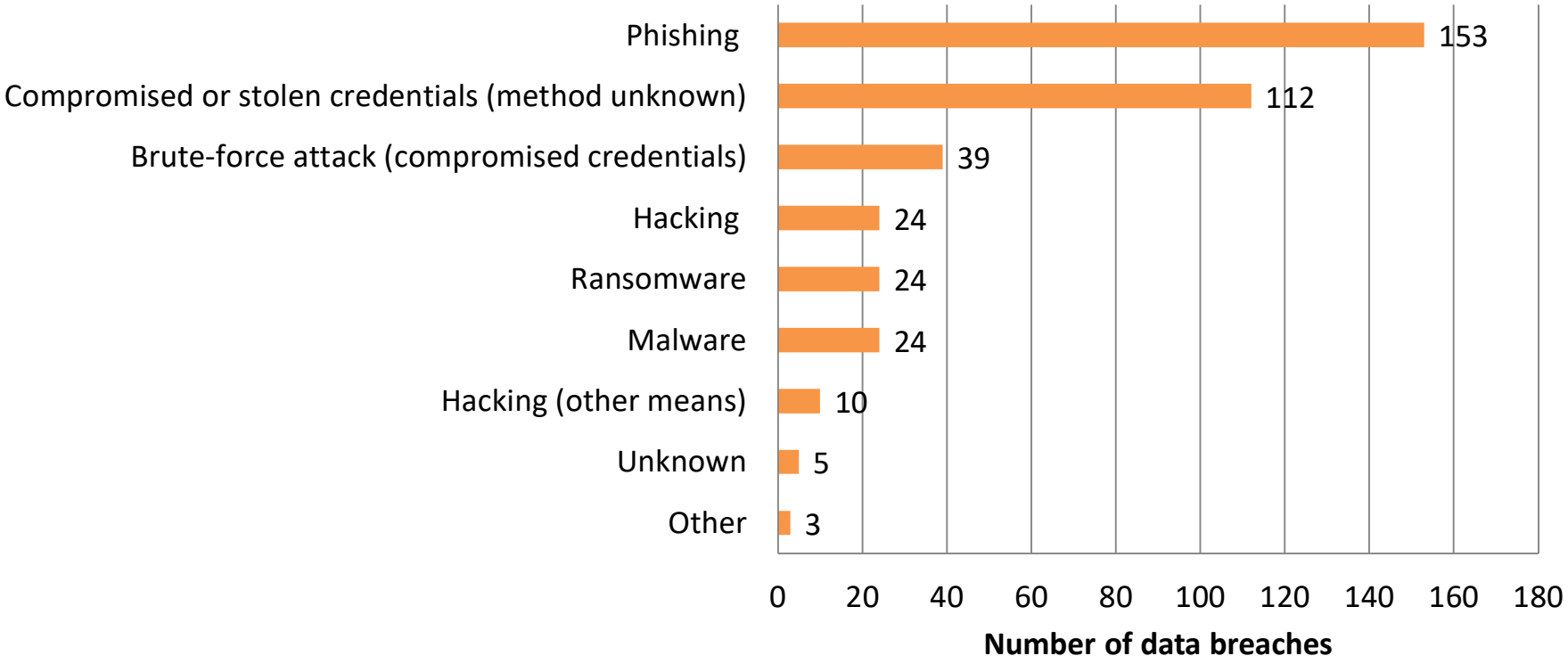


Source: Notifiable Data Breaches Scheme 12-month Insights Report, Office of the Australian Information Commissioner, 13 May 2019

The regulatory landscape

CLYDE&CO

Type of cyber incidents - All sectors

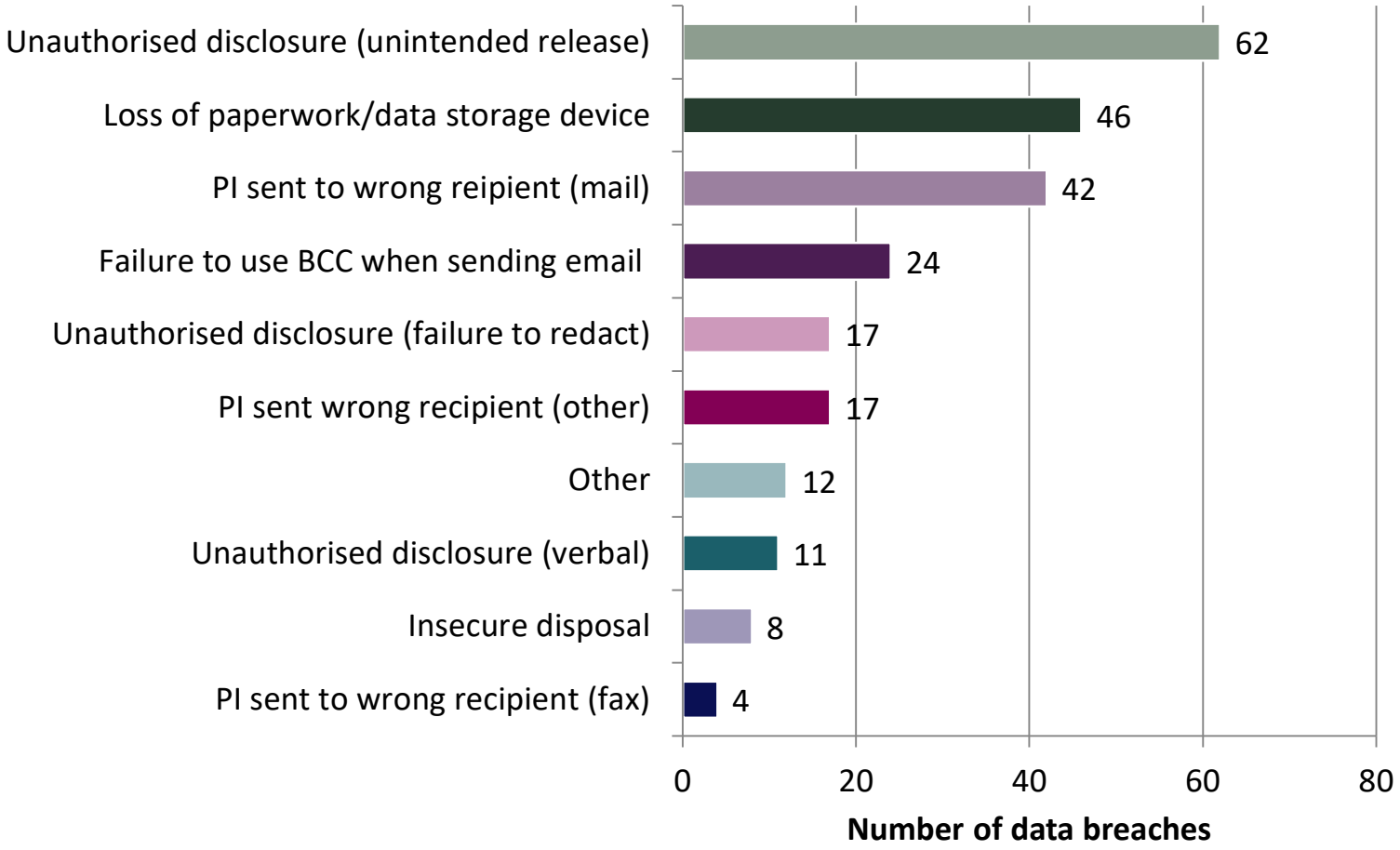


Source: Notifiable Data Breaches Scheme 12-month Insights Report, Office of the Australian Information Commissioner, 13 May 2019

The regulatory landscape

CLYDE&CO

Human error breaches – all sectors



Source: Notifiable Data Breaches Scheme 12-month Insights Report, Office of the Australian Information Commissioner, 13 May 2019

The regulatory landscape

CLYDE&CO

Regulation and enforcement

- **The OAIC's approach has been to drive awareness of entities' obligations and the causes of data breaches to support better practices**

- **Many organisations have been proactive in engaging with the OAIC**

- **But how should data breaches be regulated?**

  Collaboration or regulatory stick?

Key actions by the OAIC

- issued a direction to compel notification where it uncovered a failure to notify individuals
- conducted regulatory enquiries to ensure breaches were contained and rectified, and that measures were implemented to prevent reoccurrence
- can investigate an entity's compliance with the Australian Privacy Principles (APPs) on the Commissioner's own initiative
- currently examining notices, policies and consent

The regulatory landscape

CLYDE&CO

OAIC 12 Month Report – Best practice tips

The OAIC expects organisations to act on the risks highlighted in their reports and to employ the following best practice tips:

1. **Training**
   Staff must be trained to protect their devices and accounts.

2. **Preventative technologies and processes**
   Invest in better security measures including MFA, encryption and secure data technologies.

3. **Preparation**
   Ensure you have data breach response plan that provides practical guidance in the event of a data breach and that it has been tested.

4. **Assessment of harm**
   Ensure data mapping has been conducted to ensure you are able to make a prompt and thorough assessment if a breach occurs.

5. **Post-breach communication**
   Put the individual first. Communicate in plain English and provide practical information that helps people to mitigate harm.

The regulatory landscape

CLYDE&CO

OAIC 12 Month Report – Key takeaways

Harm minimisation

- Timely notifications
- Plain English notifications that explain key risks and how they can mitigate them

Navigating multi-party breaches

- Improved coordination where organisations hold information jointly

Managing multi-jurisdictional breaches

- Identify how a jurisdictional breach would be best managed to protect consumers, noting the different global notification thresholds which apply

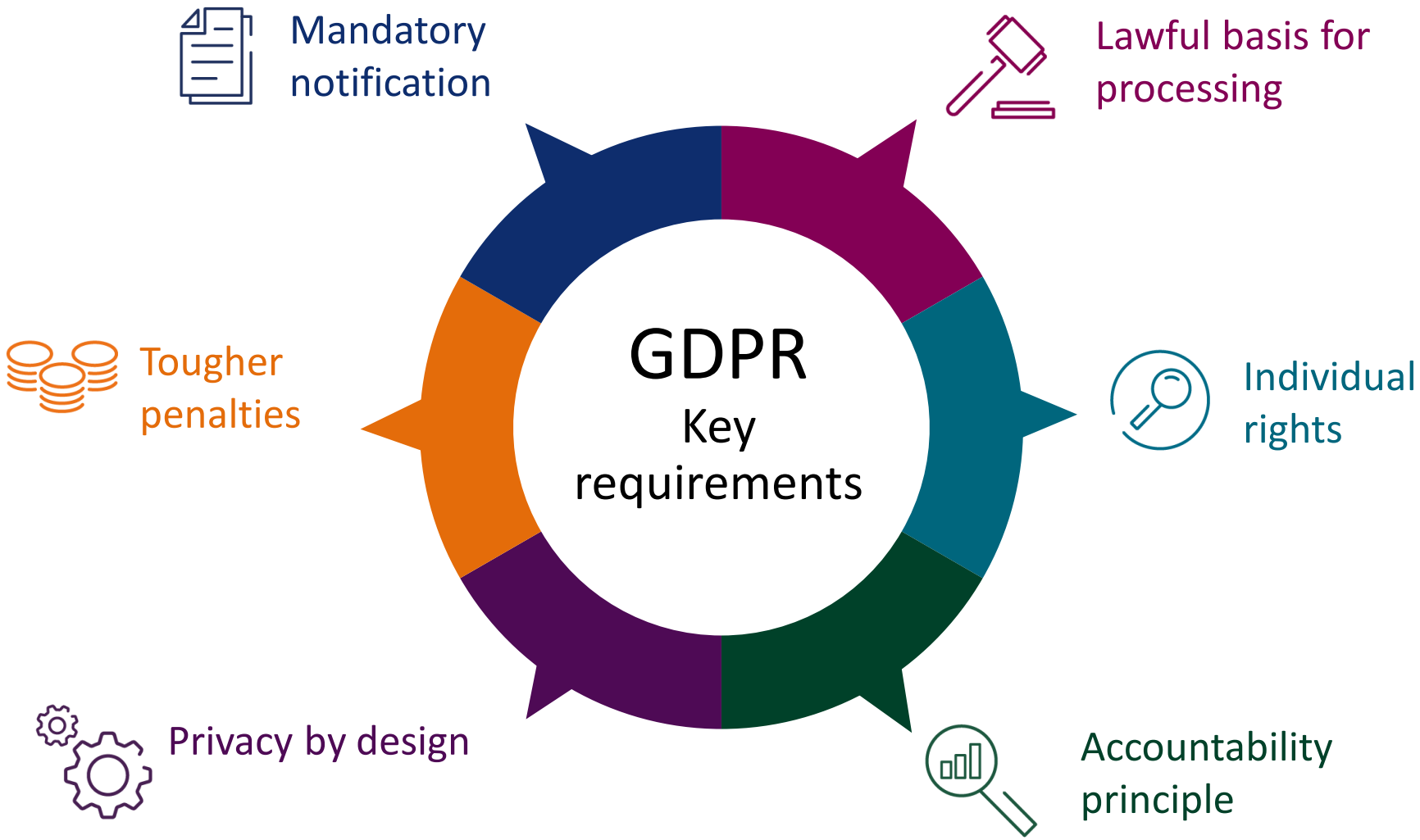
Move beyond compliance

- Take proactive steps and invest in preventative technologies to minimise risk

GDPR

CLYDE&CO

Key requirements



GDPR: Statistics

CLYDE&CO

12 month review

Over **89,000 data breach notifications** have been logged by EEA supervisory authorities

144,000 queries and complaints

56 million euros in fines as at February 2019

- 50 mill to Google in January 2019
- Supervisory Authorities from 11 EEA countries have imposed fines

Enforcement

- Active regulators include the French regulator (CNIL), the Irish regulator (the DPC), and the UK Information Commissioner (ICO)
- ICO recently announced its first GPDR action, ordering the HMRC, the UK tax authority to delete 5 million voice records that had been collected without valid consent

Source: European Data Protection Board - https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en

GDPR: Key Trends

CLYDE&CO

12 month review

Complaints mostly relate to access requests, right to erasure, unfair processing, disclosure, unwanted marketing and employee privacy

Key complaint to the CNIL

- Dissemination of data on the internet (373 requests for delisting links and significant volume of requests for deletion of names, contact details, comments, photographs, videos and accounts)

Key complaints to the DPC:

- Access Rights **30%**
- Multinational complaints – others – **22%**
- Unfair processing of data – **15%**
- Disclosure – **11%**
- Electronic Direct Marketing – **6%**
- Failure to secure data – **2%**
- Unauthorised access - **<1%**

Notable increase in queries and complaints relating to the use of CCTV, dashcams and bodycams (DPC, CNIL)

Increase in the use of the right to data portability by bank customers and online content services users (CNIL)

Complexity in the queries and complaints received post-GDPR due to increased awareness (DPC)

GDPR: Lessons learned

CLYDE&CO

12 month review

- ✓ **Quick response and notification may help to reduce punishment**
- ✓ **Deliberate conduct that is non-compliant may result in higher penalties**
- ✓ **Ignorance has no bearing on fines**
- ✓ **Avoidance of costs is no excuse for non-compliance**
- ✓ **Data subjects have heightened awareness of their individual rights**

GDPR: Territorial scope

CLYDE&CO

Article 3 of the GDPR

In November 2018, the European Data Protection Board (**EDPB**) released **draft guidelines** about the territorial scope of the regulation

Key takeaways

- "Stable arrangement" is the threshold test for whether there is an "establishment" in the EU (Article 3(1))

The requirement that data subjects be located in the EU must be assessed at the moment when the relevant trigger activity takes place. (Article 3(2))

An element of targeting individuals in the EU is required. (Article 3(2))

Source: *https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf*

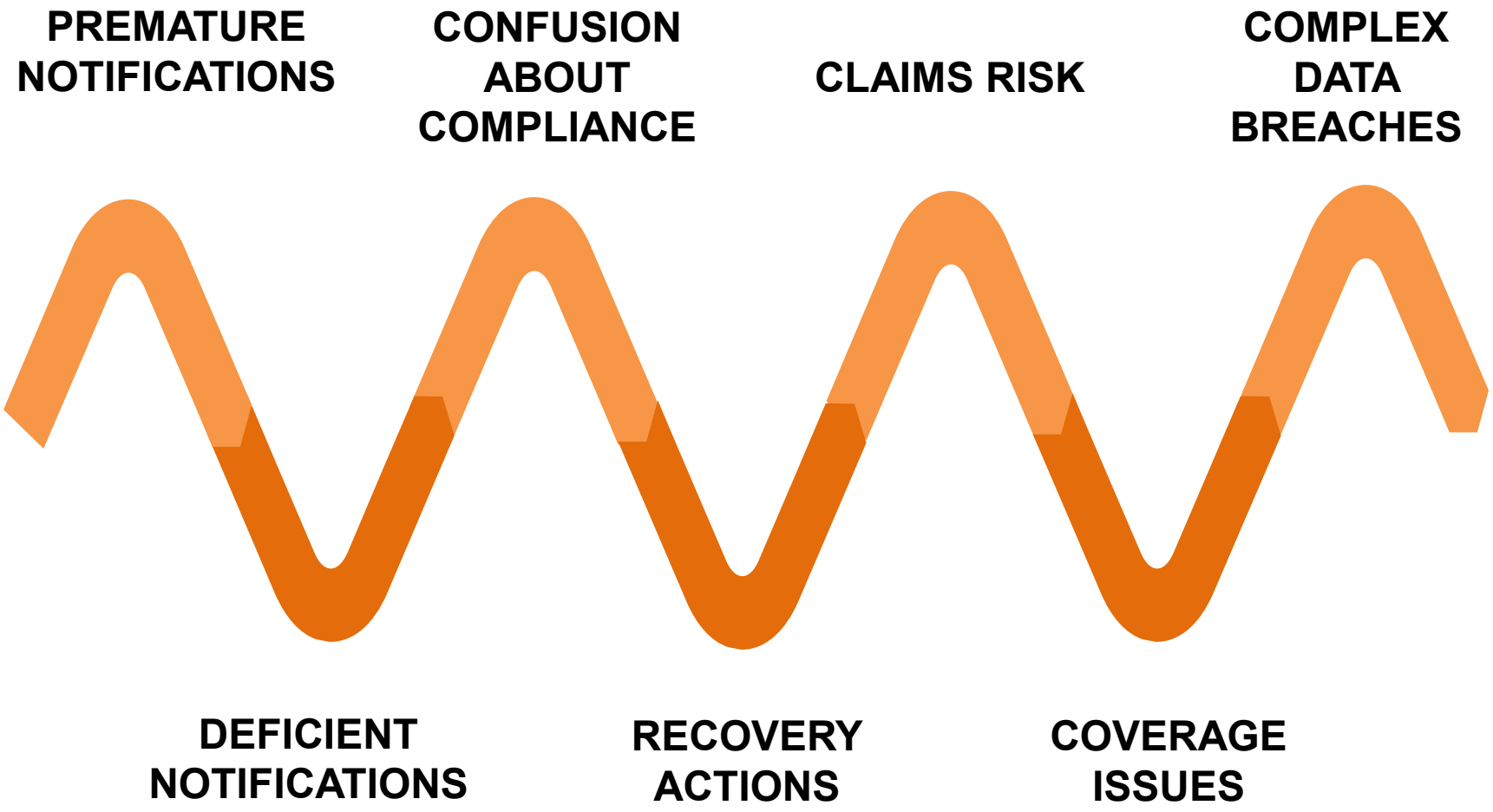
GDPR: Misconceptions

CLYDE&CO

- ✗ Consent is the only lawful means of processing data
- ✗ Breaches will result in large fines
- ✗ Small businesses are exempt
- ✗ All businesses require a Data Protection Officer

Key trends

CLYDE&CO



Business Email Compromise

CLYDE&CO

Common issues

- **Incident Response**
  - Audit logging not enabled resulting in lack of forensic evidence
  - Failures by organisations to maintain logs or preserve affected mailboxes after incident
- **Privacy Implications**
  - Assessment of PII in whole mailbox takes time
  - Need to work with the client and forensic vendors closely to narrow the scope of PII for review and conduct risk of harm assessment in preparation for notification
  - An assumption that the whole mailbox has been compromised can result in notification fatigue and increased costs and likelihood of complaints

Ransomware

CLYDE&CO

Common issues

- **Incident Response**
    - System rebuilds resulting in removal, alteration or lack of forensic artefacts
    - Competing tensions to restore operations quickly to mitigate business interruption losses
    - Inadequate backups
    - Failures to consider privacy implications after files decrypted
- **Privacy Implications**
    - The integrity or availability of evidence has a significant impact on the costs, utility and outcome of forensic investigations and resulting regulatory investigations or claims

How can you prepare?

CLYDE&CO

- Review **IT systems management and security procedures**
- Undertake a **NDB / GDPR application assessment**
- Review **insurance requirements**
- Review **third party contracts** - understand both parties' obligations
- Undertake **data mapping and audit processes**
- Develop **Incident Response Plan** and build in insurance process
- Once plans are developed – undertake **scenario testing**
- Develop and implement employee awareness training and continual education

Future trends and issues

CLYDE&CO

Changes in legislation

Changes in attack vectors

Critical infrastructure risks

Advancements in AI

Individual right to Privacy

Review of surveillance laws

Introduction of the Human Rights Act

Questions and Answers

CLYDE&CO

Get in touch with our team

CONTACTS

Matthew Pokarier
Partner, Brisbane
E: matthew.pokarier@clydeco.com
T: +61 7 3234 3001

Stefanie Luhrs
Senior Associate, Brisbane
E: stefanie.luhrs@clydeco.com
T: +61 7 3234 3006

WHAT TO DO WHEN THINGS GO WRONG

Cyber incident response hotline
+ 61 2 9210 4464

Emergency response email
cyberbreach@clydeco.com

HOW CLYDE & CO CAN HELP?

PRE-INCIDENT

INCIDENT RESPONSE

POST-INCIDENT

CLYDE&CO

440
Partners

2,500+
Legal professionals

4,000+
Total staff

50+
Offices and associated offices worldwide