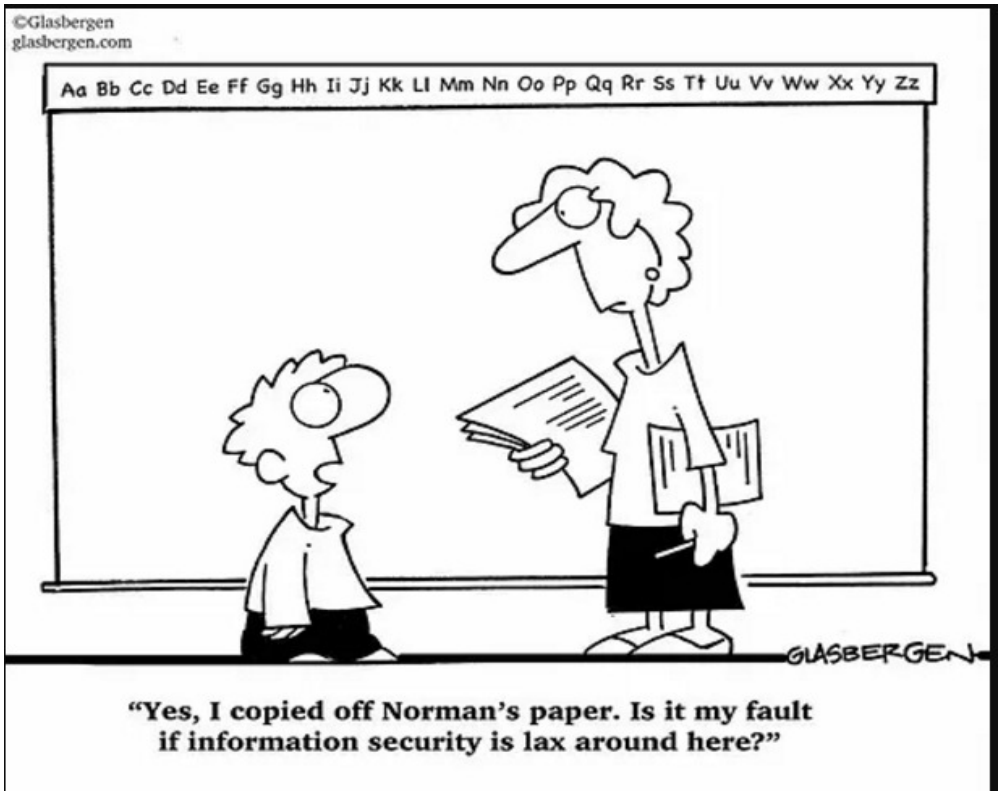
©Glasbergen
glasbergen.com
Aa Bb Cc Dd Ee Ff Gg Hh Ii Jj Kk Ll Mm Nn Oo Pp Qq Rr Ss Tt Uu Vv Ww Xx Yy Zz
GLASBERGEN
"Yes, I copied off Norman's paper. Is it my fault if information security is lax around here?"

Crime and Corruption Commission
QUEENSLAND

RELEASE OF CONFIDENTIAL INFORMATION

WHAT HAVE WE LEARNT?

APSACC NOVEMBER 2017

Presented by:
Craig Hawkins
Operations Coordinator
Corruption Operations

Misuse of Information

- It is a prevalent topic of allegation against QLD public sector employees (between 7 and 11.5% of complaints received per year)
- Has been and remains an area of priority for QLD CCC
- 2/3 complaints are about police
- Investigations regarding confidential information often result from investigations initially commenced into unrelated allegations.

Release of Confidential Information

- **Information leaks**. The unsanctioned disclosure of official or sensitive information to people who are not authorised to receive it.
- **Green lighting.** When a corrupt or compromised official informs a person when or where it would be safe to engage in illicit activity without fear of detection.
- **Tip-offs.** When a corrupt or compromised official warns criminals of current or planned law enforcement activity.

Release of Confidential Information

- **Significance of the issue**
  - Breaches privacy
  - Can constitute a criminal Offence (*s408E (1) &/or (2) and s92A of the Qld Criminal Code)*
  - Compromise law enforcement activities
  - Erode public confidence

Misuse of information – options for the CCC Qld

OFFENCE SECTION	OFFENCE	KEY ELEMENTS	PENALTY
92A Criminal Code	Misconduct in Public Office	• With intent • To dishonestly • Gain benefit/cause detriment (a) Deals with info gained in office or (c) act or omission in abuse of office	7 years
408E(2) Criminal Code	Computer hacking/misuse with aggravation	• Use restricted computer • Without consent • Causes or intends to cause • Benefit or detriment	5 years
408E(1) Criminal Code	Computer hacking/misuse	• Use restricted computer • Without consent	2 years
10.1 Police Service Administration Act	Release of Information	• Police officer • Discloses info • Gained through position/employment	100 PU ($12,190)

Important evidentiary points to prove elements of s408E

- A ‘person’ who uses:
  - Proving:
    - Actual Employment/graduation dates/oaths of service/registered number/user ID
    - Actual position/posting at relevant time
    - That defendant was actually working at relevant times (rosters/payslips/ITAS logs/occurrence logs etc, vehicle runningsheets, security door swipe registers)

Important evidentiary points to prove elements of s408E

- Use of the computer:
  - Source – data activity reports
    - In its raw state is the evidence
    - This should contain relevant log on/off details and accesses only
    - Evidence given by someone who can give evidence of how to read/translate
    - That information needs distilling into a statement/table form plus a summary (as an evidentiary aid)

Important evidentiary points to prove elements of s408E

- Use of the computer:
  - The information in statement/table form – needs to detail:
    - User ID
    - Log on/log off times
    - Search terms used
    - Each relevant record viewed, tab change performed, records printed etc

“Restricted Computer”

- Required to Prove:
  - That the program is stored on the Computer
  - A code is required for access
  - The defendant has a specific code User id/password)
  - The controller has policies and procedures dealing with password control (user ID and password management and warning screen/s)

Without Consent of the Controller

- The controller's evidence:
  - Limited consent to access system
  - Limitations placed on consent and how
    - Standard of Practice for org
    - System information Manuals
    - Screen Warnings at log on
    - Code of Conduct or OPM
    - Policies re conflict of interest
    - Access details given to controller to make comment on

Important evidentiary points to prove elements of s408E cont'd

- Restricted computer:
  - How is it restricted? (evidence to be given by the controller)
  - Required to prove:
    - Data in program stored on departmental computer
    - A code to access (unique user name and password)
    - Defendant has a code to access
    - Controller has policies & procedures dealing with password control (i.e. User ID & Password Management Standards and warning screens)

Important evidentiary points to prove elements of s408E cont'd

- Training received by Defendant
  - Recruit/probationary induction profiles
  - Training programs – including training transcripts
  - Relevant courses
  - Emails – Circulars – Directions from Senior Management /Commissioner

Case Officer

- Details of investigation including:
  - Records viewed (ie. Occurrences, person/vehicle details, screen shots of searches undertaken and results, ITAS logs, hard copy and electronic diaries, emails and attachments.
  - Obtains statements from all relevant witnesses
  - Preparation of Briefs Of Evidence

Conclusion

- Similar to other jurisdictions, unauthorised access and the release of confidential information remains an issue for the Queensland Police Service and public sector agencies
- Agencies need to remain vigilant regarding access to restricted and confidential information
- Agencies need to ensure there are sufficient policies, procedures and training in place and clearly communicate those expectations to staff

Thanks for Listening
Any Questions?

Stay up to date

Subscribe for news and announcements
www.ccc.qld.gov.au/subscribe

Follow us on Twitter
@CCC_QLD