actlaw society

Briefcase to Cyberspace: cyber security considerations for government lawyers

ANNIE HAGGAR
PARTNER, NORTON ROSE FULBRIGHT AUSTRALIA

AMANDA WESCOMBE
SPECIAL COUNSEL, NORTON ROSE FULBRIGHT AUSTRALIA

GOVERNMENT LAW CPD MORNING, THURSDAY 24 OCTOBER

NORTON ROSE FULBRIGHT

Your Presenters

Annie Haggar

About Annie

Partner, Head of Cyber Security Australia

Annie is one of Australia's leading cyber security lawyers with a proven track record of excellence in the field of cyber security and technology law in Australia and globally, having supported multinational businesses, governments, and critical infrastructure clients on emerging cyber issues across a more than 20-year career.

Amanda Wescombe

About Amanda

Special Counsel

Amanda is a senior cyber security lawyer and a trusted advisor to private sector and government clients. At Norton Rose Fulbright Amanda's practice combines her legal, commercial, and governance experience to advise clients how to understand, prepare for, defend against, and recover from, cyber-attacks.

LawyersWeekly Australian Law Awards WINNER Sole Practitioner of the Year 2024

LawyersWeekly Corporate Counsel Awards WINNER Technology, Media and Telecommunications Lawyer of the Year 2021

LawyersWeekly Australian Law Awards WINNER General Counsel of the Year 2021

Australasian Law Awards 2021

Women in Defence Awards 2019

Extreme 2016

Lawyers Weekly Australian Law Awards 2015

NRF

OUR TOPICS TODAY:

Part 1: Foundations of cyber security in Australia
Part 2: Latest developments
Part 3: Dealing with a breach

Part 1: Foundations of cyber security in Australia

Cyber security is in the news…

The Guardian https://www.theguardian.com/technology/2023/may/02/australian-law-firm-hwl-ebsworth-hit-by-russian-linked-ransomware-attack

Australian law firm HWL Ebsworth hit by Russian-linked ransomware att

of 4TB of data including IDs, finance reports,
s and credit card details.

Ticketek Australia investigates 'cyber incident' imp
'account hold
information'

https://7news.com.au/news/ticketek-australia-investigates-cyber-incident-impacts

Canberra club members at risk of identity theft after major data breach

https://be-riotact.com/canberra-club-members-at-risk-of-identity-theft-after-major-data-breach/766616

Morning Herald

in Victorian EP

sky

OAIC

2 May 2024 | James Coleman

Report shows highest number of data breaches in 3.5 years

https://www.oaic.gov.au/news/media-centre/report-shows-highest-n...

WEB 16 Sep 2024 · New statistics from the Office of the Australian Information Commissioner (OAIC) show the number of data breaches notified to the regulator in the first half of 2024 ...

https://www.oaic.gov.au/news/media-centre/report-shows-highest-number-of-data-breaches-in-3.5-years

AFR

Cyber is our fastest growing national security threat: O'Neil

Home Affairs Minister Clare O'Neil says banks, telcos and technology providers need to to help small business and consumers fight off growing...

https://www.afr.com/technology/cyber-is-our-fastest-growing-national-security-threat-o-neil-20240705-p5jrhh?collection=p5jvkm

https://www.9news.com.au/national/personal-data-of-thousands-stolen-in-epa-breach/43587aa7-b380-4ff7-bf8a-137072a002cd

Hackers threaten to publish data from attack on legal services firm

Medibank data breach

WEB Nov 9, 2022 · At 1.20pm on October 12, from Australia's top cyber spy agency. It came with a business wants to hear. The Australian Signals Directorate...

https://www.afr.com/technology/inside-australia-s-most-invasive-data-hack-20221109-p5bwsk

NEWS

Australian Law Firm Allens Caught Up in Cyberattack

law.com/international-edition/2021/01/25/australian-law-firm-allens-caught-up-in-cyber-attack/?slreturn=2024101720132

firm's client data was compromised after a file-sharing system designed by California-

Australia port operations

ub/news-content-hub/cyber-attack-takes-out-dp-world-australia-port-operations-78518

been able to determine whether the cyber attack had compromised its own and customers' data.

iry in this ongoing investigation is the nature ...

NRF

Cyber statistics

67%

of data breaches reported to the OAIC occurred because of a malicious or criminal attack

43.6%

of submitted cyber incidents to ASD were reported by federal, state, or local governments

55%

of cyber incidents reported to OAIC involved phishing or similar methods to gain user credentials

94,000

reports were made to ASD in the prior year through ReportCyber – equal to 1 every 6 minutes

1 in 5

victims reported a ransomware attack when it occurs

30%

of data breaches reported to the OAIC occurred because of human error

527

data breach notifications were made to the OAIC between January to June 2024

$42bn

is the annual cost to the Australian economy because of cyber crime

Sources: *ASD Cyber Threat Report 2022-23*; *OAIC Notifiable Data Breaches Report: January to June 2024; AIC Crime & Justice Research 2023; Cyber crime in Australia: 20 years of in-action - Mr Nigel Phair 2021*

Part 2: Latest developments

Laws

CURRENT LAWS

- *Privacy Act (Cth)* 1988
- *Corporations Act (Cth)* 2001
- *Security of Critical Infrastructure Act (Cth)* 2018
- *Telecommunications Act (Cth)* 1997

NEW LAWS

- New Cyber Security Bill 2024 tabled 09/10/24
  - ✓ Cyber Incident Review Board (CIRB)
  - ✓ Limited use ≠ 'Safe harbour'
  - ✓ Internet of Things (IoT) security standards
  - ✓ Mandatory ransom payment reporting
- *Privacy Act* reforms tabled 12/09/24
  - ✓ Doxxing
  - ✓ Privacy policy that meets new requirements
  - ✓ Cyber incident reporting obligations update
  - ✓ New tort of serious invasion of privacy
- *Security of Critical Infrastructure Act* (SOCI) amendments tabled 09/10/24
  - ✓ New categories of critical infrastructure assets = includes secondary assets that hold critical data and relates to the primary asset
  - ✓ Telecommunications Act security requirements transitioned into the SOCI Act
- *Intelligence Services Act* amendments to allow for limited use sharing

NRF

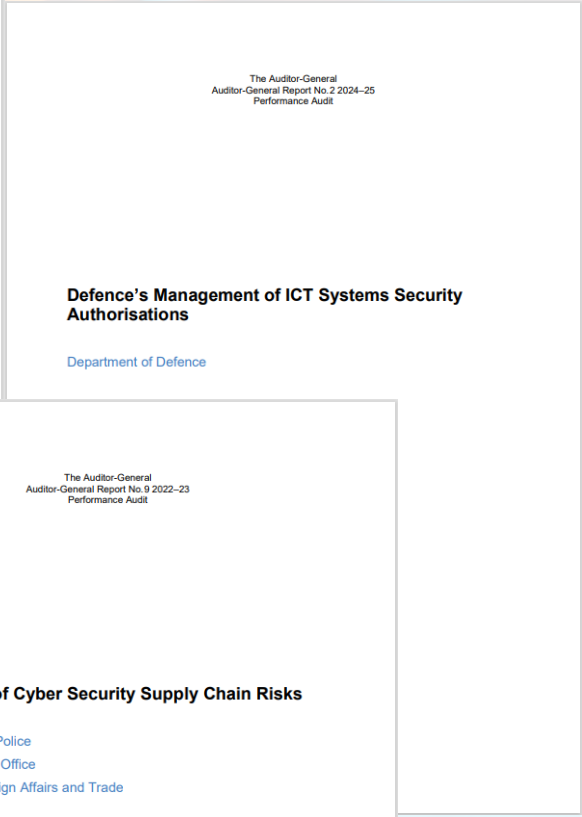
Sources: *Parliament of Australia - Cyber Security Bill 2024*

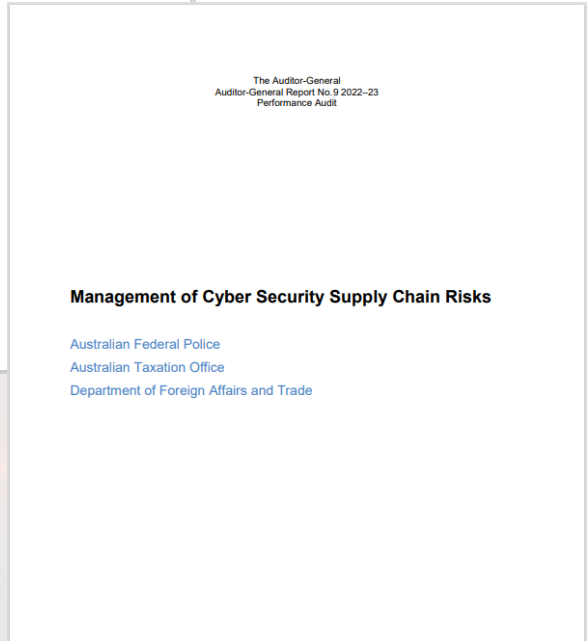
Regulatory and legal developments

	OPTUS [September 2022]	MEDIBANK [October 2022]	LATITUDE [March 2023]	HWL EBSWORTH [April 2023]
REGULATORY ACTION	*Australian Communications and Media Authority* (**ACMA**) • announced investigation [11 October 2022]: issued $1.5m penalty [6 March 2024] • filed FCA proceedings [22 May 2024]: 3.6 million x $250,000 per penalty = potential $900 billion *OAIC* • announced investigation [11 October 2022]	*Office of the Australian Information Commissioner* (**OAIC**) • filed proceedings in the Federal Court of Australia (FCA) [14 June 2024]: 9.7 million each x $2.2 million each contravention = potential $21.5 trillion *Australian Prudential Regulation Authority* (**APRA**) • imposed $250 million capital adequacy requirement [27 June 2023]	*OAIC* and *The New Zealand Office of the Privacy Commissioner* (OPC) • commenced a joint privacy investigation [10 May 2023] • first ever joint commissioner investigation	*OAIC* • commenced investigation [21 February 2024]: response to data breach notification 8 May 2023
LEGAL ACTION	*Slater & Gordon* • filed a consumer class action in the FCA [21 April 2023] • over 100,000 participants	*Phi Finny McDonald* and *Quinn Emanuel Urquhart & Sullivan* • commenced shareholder class action [29 March 2023] *Slater & Gordon* • filed consumer class action in the FCA [4 May 2023] • joined by *Baker McKenzie [*1 August 2023]	*Gordon Legal and Hayden Stephens & Associates* • announced investigations into potential legal action [28 March 2023] • lodged a complaint with OAIC	*National Justice Project* • given notice to represent 12 NDIS participants in a class action [3 September 2024]

Australian National Audit Office

- **2022 – Management of Cyber Security Supply Chain Risks**
- **2024 – Management of Cyber Security Incidents**
- **2024 – Defence's Management of ICT Systems Security Authorisations**





Part 3: Dealing with a breach

Who is attacking Government entities?

State-sponsored attacks

Hacktivists

Cyber criminals

Insider threats

State-sponsored attacks are happening right now.

Chinese hackers access US telecom firms, worrying national security officials

By Sean Lyngaas and Evan Perez, CNN
3 minute read · Updated 8:24 AM EDT, Sun October 6, 2024

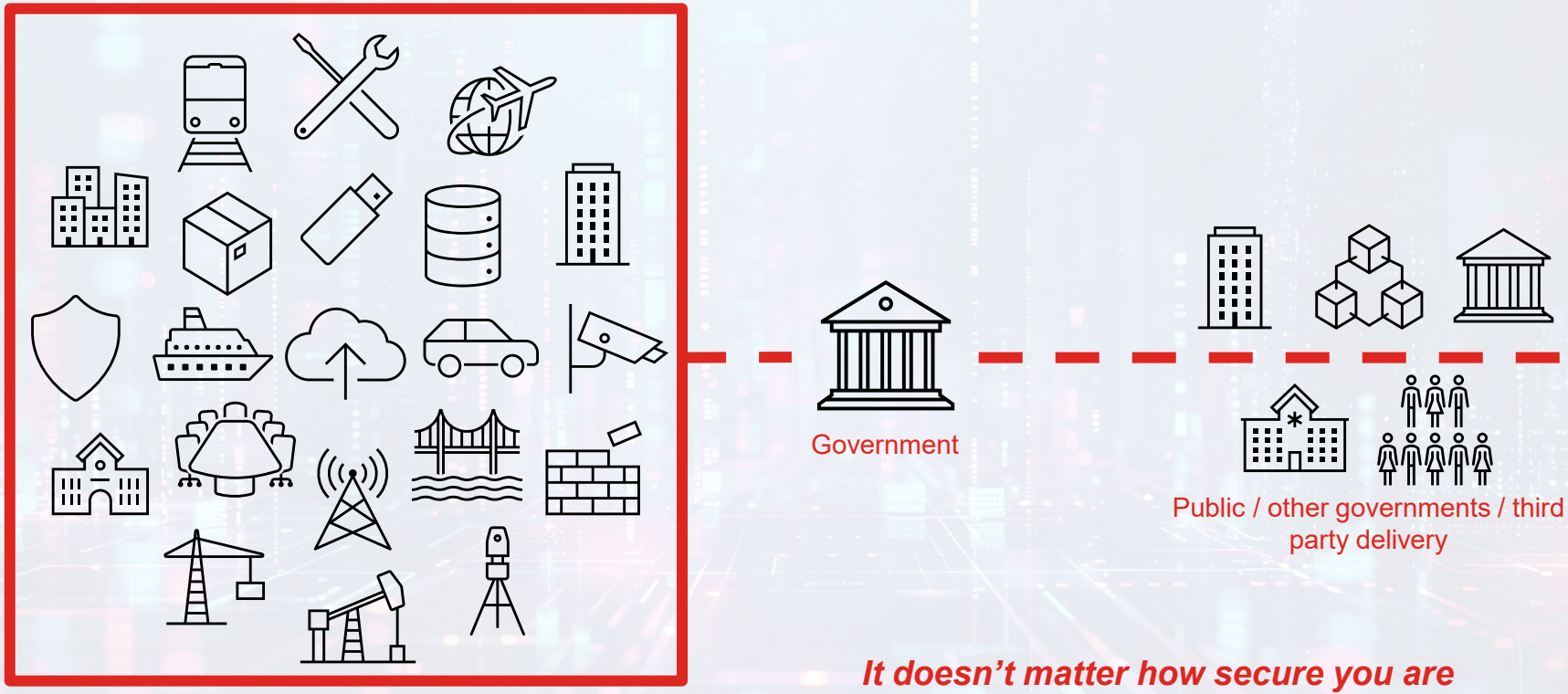
Chinese hackers spent 5 years waiting in U.S. infrastructure, ready to attack, agencies say

The report is one of the first public indications that Chinese hackers have had years of access to U.S. infrastructure.

Impacts of a cyber incident on government

- Breaches
- Loss of Trust
- Funding Scams
- National Security
- 5th Domain of War
- Waste of Public Money

Attack type: Supply Chain (or “indirect”) Attack



Government Supply Chain

Government

Public / other governments / third party delivery

It doesn’t matter how secure you are if you don’t secure your supply chain

NRF

Direct

What kind of breach?

Indirect

CISO calls

- Impact on systems
- Level of data impacted
- Regulations
- Investigations
- Briefings
- Notify impacted people

Direct

What role does legal play?

Indirect

Legal role

- Impact on systems
- Level of data impacted
- Regulations
- Investigations
- Briefings
- Notify impacted people

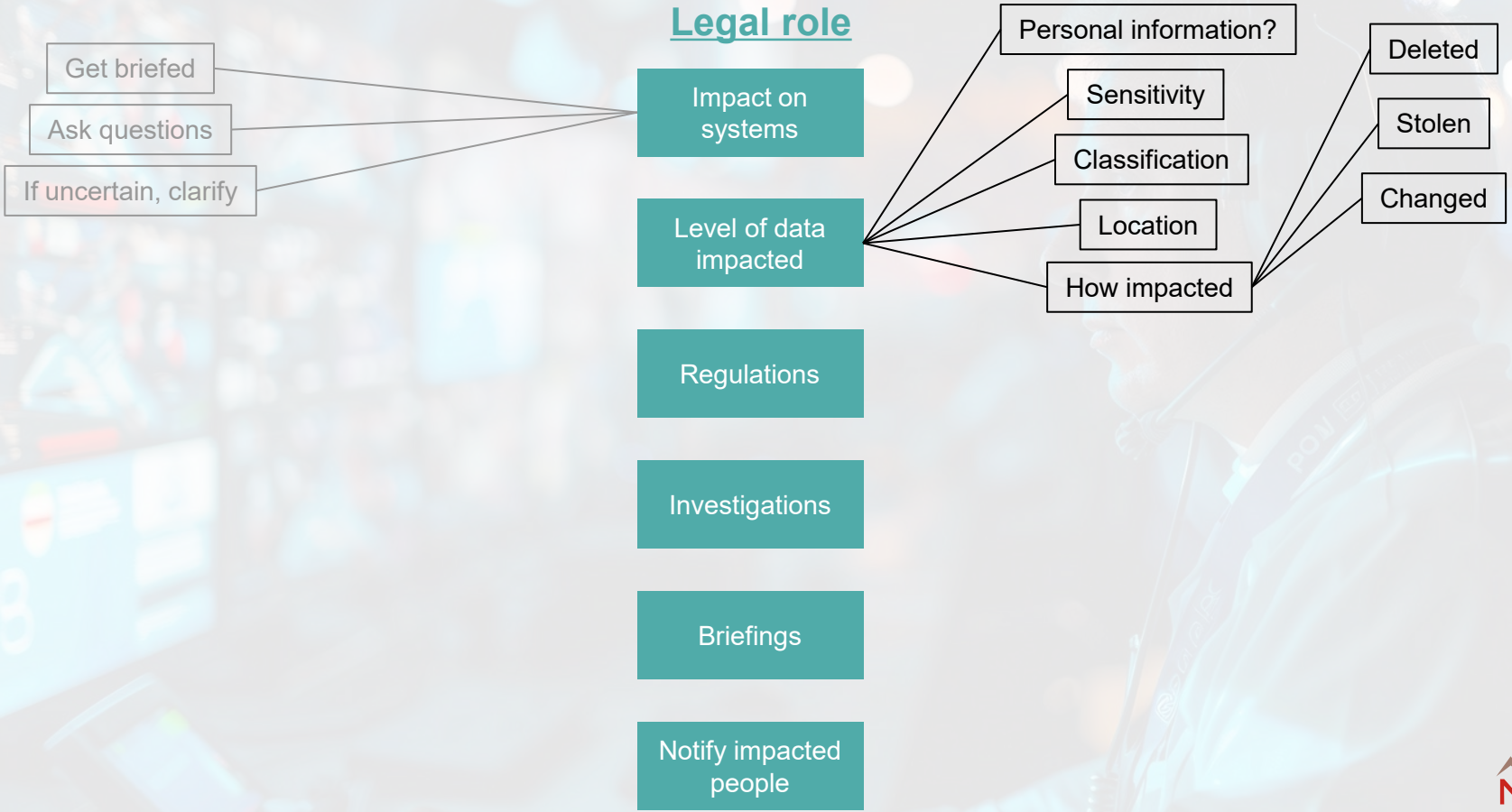
What role does legal play?

Direct

Indirect

What role does legal play?

Direct **Indirect**



What role does legal play?

Direct **Indirect**

Legal role

- Impact on systems
  - Get briefed
  - Ask questions
  - If uncertain, clarify
- Level of data impacted
  - Personal information?
    - Deleted
    - Stolen
    - Changed
  - Sensitivity
  - Classification
  - Location
  - How impacted
- Regulations
  - Who?
  - What?
  - When?
  - Where?
  - Why?
  - ASD
  - OAIC
  - ASIC
  - Other regulators
  - SONS/SOCI
- Investigations
  - Drafts
  - Reviews
  - Commissions
  - Tracking/Monitoring
- Briefings
- Notify impacted people

What role does legal play?

Direct

Indirect

Legal role

- Get briefed
- Ask questions
- If uncertain, clarify

Impact on systems

- Who?
- What?
- When?
- Where?
- Why?

Regulations

- ASD
- OAIC
- ASIC
- Other regulators
- SONS/SOCI

- Drafts
- Reviews
- Commissions
- Tracking/Monitoring

Level of data impacted

- Personal information?
- Sensitivity
- Classification
- Location
- How impacted

- Deleted
- Stolen
- Changed

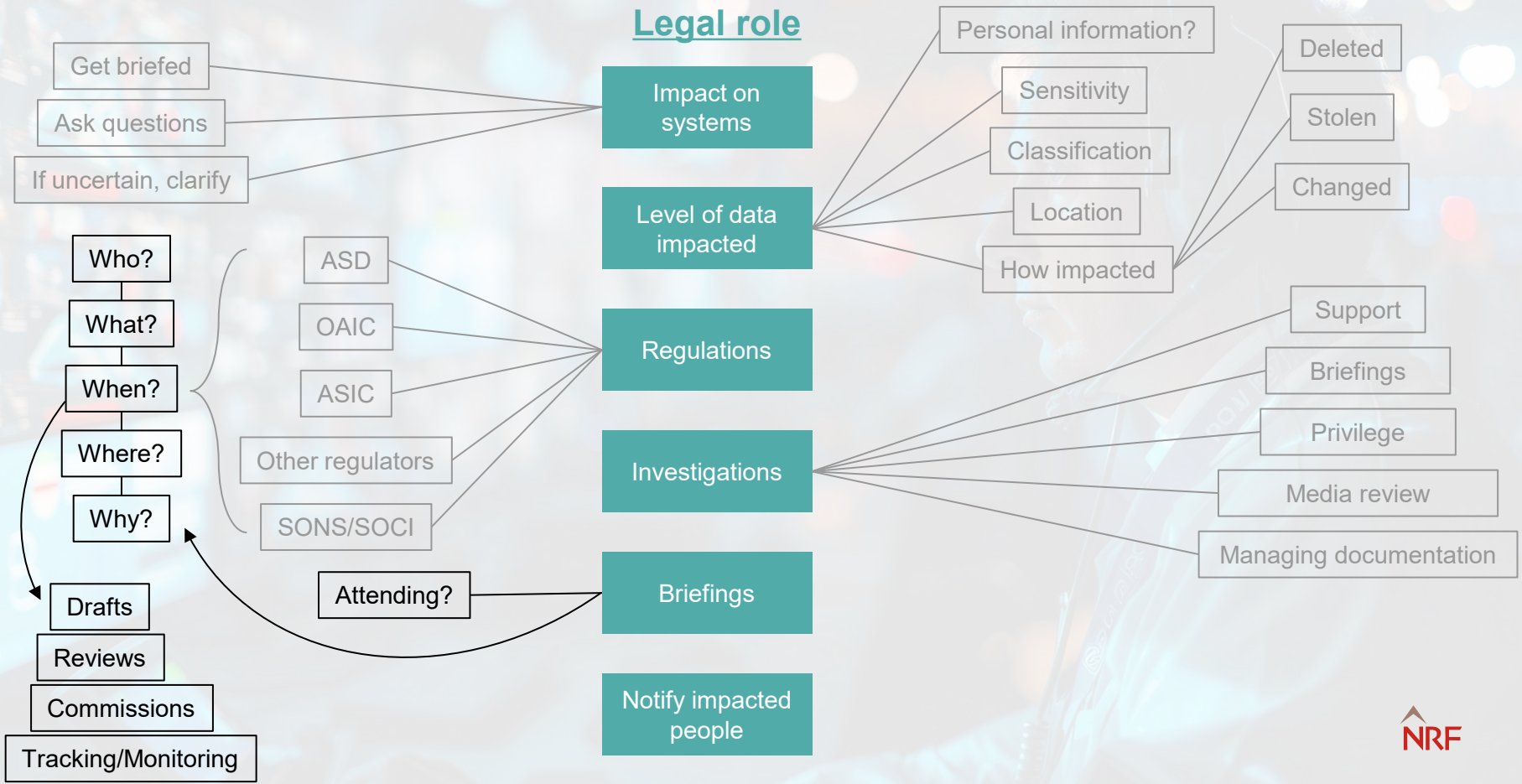
Investigations

- Support
- Briefings
- Privilege
- Media review
- Managing documentation

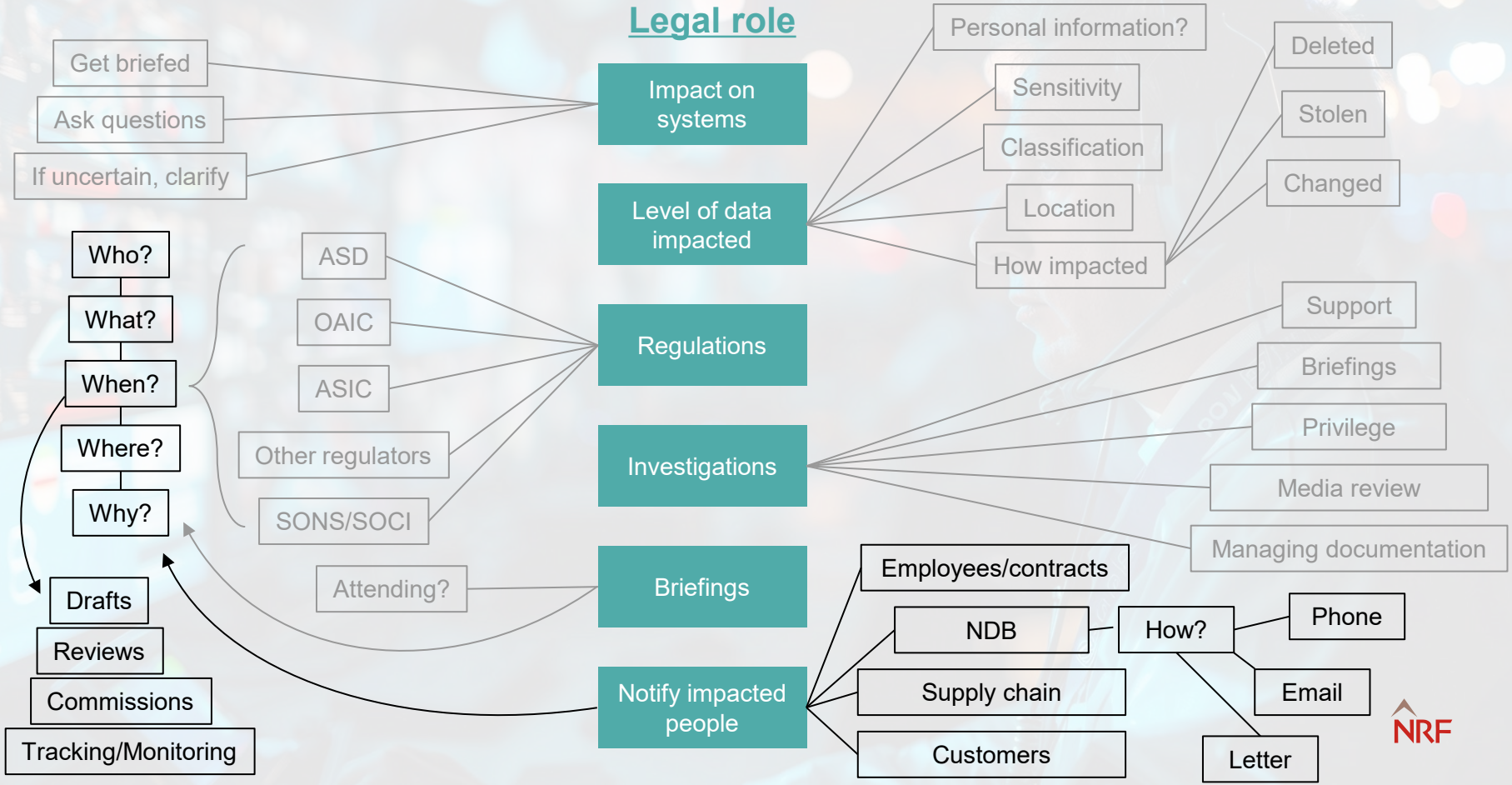
Briefings

Notify impacted people

Direct What role does legal play? Indirect



Direct What role does legal play? Indirect



Prepare for a breach

- IR Plan for Entity
- Legal's Incident Response Plan (**IR Plan**) needs:
  - ❑ Is there one? Where is it stored? When was it last updated?
  - ❑ Where are your key delegates? Where is the list? Where are their contact details stored?
  - ❑ Have you pre-drafted any regulatory communication? Work with the comms team.
  - ❑ Where is your contact database for all like Notified Data Breach (NDB)/Supply chain?
  - ❑ Have you extended or got expertise across cyber tech, legal, or support?
  - ❑ Have your legal + technical experts been retained and cleared?
  - ❑ Do your key supply contracts include requirements to assist?
  - ❑ Who are your key decision makers for reporting a data breach?
  - ❑ Do you have a plan for responding to ransom payment demands?
  - ❑ What level of disclosure or authority has been granted to your key decision makers?
  - ❑ How will you protect privilege?
  - ❑ Is there a media plan or response incorporated into the IR Plan?

Questions

NORTON ROSE FULBRIGHT

Law around the world

nortonrosefulbright.com

Law Society of the Australian Capital Territory
Level 4, 1 Farrell Place, Canberra City ACT 2601
Phone 02 6274 0333 | memberconnect@actlawsociety.asn.au

actlawsociety.asn.au