-Cop?

Metrics

- WP spk Pak re 'interconnectedness' ToR.

- Fluid, mobile staff, taskforces
- Complex environment for small organ^

Pak - Δ's in last 3 years (MoG)
- From 700–800 staff to 2,500. ✓✓
- Pace of Δ that occurs ⇒ housekeeping (capacity to build capability) never opportunity to 'breathe'.
- Nov new MoG ⇒ teams going out.

RS - Protective Security Manual ⇒ now PSPF
⇒ each agency 'protocols'

PS - applic^ : PSPF compliance process : we rank highly on compliance against measures,
- don't score behaviours & cultural piece.

- Assessment resets every 12 months.

RS q^ - does report go via Operations Committee? (Yes)
- Security reports 3 times year
⇒ 2 sec. updates plus PSPF report.

s33(a)(i)

⇒ lots of waivers & backlog created for clearances for other depts.
Waivers : citizenship waivers, etc.

J - PSPF - 'must' or 'should'; rest are discretionary

RS - need something 'purpose designed' for each dept.

WYW - Security implic^ ?

PS - Yes. Represent^ from s22 [redacted] team.

- Always engaged in terms of Secure Areas. s 33(a)(i) [redacted]

① (- Codesign process) - bet^ areas (fiscal, cabinet) with Sec. requirements.

- few people working all day on secure system s 33(a)(i) [redacted]

∴ provide access to secure areas.

Storage - either there already or will be allocated.

s 33(a)(i) [redacted]

PS ① limited/restricted 'codesign'

s 33(a)(i) [redacted]

S - Once WYW in place, what additional guidance?

PS - not much. But opportunity.

Storage requirements & - Digitising old material (which should have been archived).

S - "opportunity"

- incident ⇒ gets people's attent^ } opport to address behaviours

+ WYW transition

Chat with Yael

2013 'set' relevant to then ; & what applies now.

YC - Cab process = life cycle.
- procedures set out what you do in particular point of chain.

- two areas : prep & (.
Cab ops & submissions team

logistics & handling & distrib^n of Cab Material
- work with all/any dept @ each stage (pre ED, ED, etc)
→ distribute finals

deal with all/others of subs & advising policy officers in PM&C.
⇒ giving advice of compliance & timing

→ Exec : work with Cab Sec re scheduling.
- Cab committees coming up.
→ locking down meetings ; prepare packs, etc.

· Cabinet plus 10 Cab. committees

Plus Exco, FOI, appointments etc process that feed in to Cabinet...
↓ 2 officers
↘ 1 officer.

→ Fed Ex canal (fortnightly)
⇒ papers sealed, etc.

—

[redacted]

FOI – managed by Gov Div^n (FOI section; own team that farms out requests & seeks advice)
- incoming FOI requests.
- frequently involve Cab or Cab. material,
- one person in Cab Div^n to review requests, & [illegible]
- any appeals ⇒ bumped up to SES to review.

andling, tracking

- protocols in place for confidential info.
- Cab Div^n doesn't keep official advice?,
⇒ PM&C response to claim is Gov Div^n.

- get to see FOI request.

Does Cab Div^n know where every Cab document is @ every point in time

- Yes.
- Need to check what Gov Div does with Cab Div response. Cab Div holds in Sharelinks but not sure how Gov Div^n handles, prints responses.

s 33(a)(i)

[redacted]

- document management & dist^n
- checking where in Cab Manual.

YC – Stocktake : used internally & externally (Ministers, dept & agencies)

RS – aware of every copy?

YC – where gone & who holds it?

s 33(a)(i)

S - process for induct°

C - orientation pack.
- (last version in RS's pack.)

? - lot of staff movement? Retention?

YC - train new staff on 'bits' of system
- Cabinet training.
- Notetaking.

| tailored to what others will be doing.

- rely on dept training for general training (eg security & fraud) & use of online modules.

K - check what training & modules in order to access various systems.

- More training on what you done when you've finished your job? : what to do with working documents.

| Separate to process around

Δ of govt & archiving of others documents.

RS - when do you know the job is done.

YC - clean up days, calendar around work hygene. esp around exit points.

Follow up on key sales issue & problems with new starters.

P - q° of what is happening to documents; YC auditing sales in Cab Div°.

RS – lessons learned ; what could review do?

s 33(a)(i)

- Cab Div' audit on Sharehub to check paper classif"

s 33(a)(i)

How do we help people create digital files & classify them correctly?

- pop ups @ creation in word? Excel?

But still won't predict against malicious behaviour.

NR – tensions re timelines bet" subs, EDs And giving enough time

[redacted]

BETA

-desensitised to security.

-effective ~~re~~ engagement → compliance.

Bob - +ve incentives around security. (*)

demerit points akin to drivers' licence.

- No systematic way to incentivise people.
- Training 'non-targeted' to groups of people.
  - lack of face to face.
  - not tailored for staff; TC received training when MoG'd A ↓ was piloted @ AP05 level. ∴ Switched off. Training has to resonate with staff.

Seek BETA to work with LAD, Security.

-Bob: can look @ training to help redesign.

s 33(a)(i) [redacted]

⇒ rewarded for performance & prod'y; not security awareness

s 33(a)(i) [redacted]

MEETING WITH NATHAN [redacted] s22

- Reports to Exec Board (on incidents) on ½ly basis
  Reporting & Board engagement can be sporadic.
- Metrics
- Interface - linking platforms.

- Gaming & phishing (& hacking) exercises

Q° of integration with Part [redacted] s22
- skill accred° for Level 2.
- more collaboration in past. [redacted] s22 for ASAs in 8(2) yrs.

How connected? (*)

Moved briefing to e-learning back (used to be face-to-face for new staff with ASA).

- part of one PMAC. [redacted] s 33(a)(i)

[redacted] s 33(a)(i)

(*) under PSPF.
- 100% focussed on WoG policy.
- own critical infrastructure. (protected network)

[redacted] s 33(a)(i)

Training - [redacted] s22 & co design.
Eg travel. [redacted] s22 always up re digital vs physical security

Effectiveness of modules: [redacted] s22 - move to e modules
⇒ no upswell in incidents
2017 - 10 security incidents (severe)
- very good by comparison to other dept.

s22 [redacted]

s22 [redacted] Nathan – no friendly partner for risk assessments
- ASD rarely providing proper advice.

s22 [redacted] – more connected with other cohorts ; more natural than ASA network,

WoFG CIO group ⇒ proxies sent ⇒ too many achan ideas ⇒ bogged down

∴ strong need to share risk assessments.

IC – ASD much to do in this space?

Under ISM – all responsible. No-one driving but there is a strong authic.
(not so obvious for ASA network).

ISM – 1036 controls (must & shoulds)
– audit document

s22 [redacted] & Nathan ; prefer clarity in black & white,

BJ: Not in PSPF.

s22 [redacted]

Ric – does cyber risk crowd out old fashion security.

Nathan – every 6 months, either Annie or all round audit.
– four audits last year.

s 33(a)(i)

[redacted]

Alistair McKibbon – internal champion

– motivated dept to move into other spaces

[redacted]

Onboarding Access

s33(a)(i)

[redacted]

Ricq^:

Compliance around ISM, responsive overlay which leads to followed sol^ which leads to better f'work/culture. Also point about McKibbin re Champions, plus networking. (informal CoP, ITSA (IT Security Adviser) network - good profile w'cos cyber is big.

Emergency Management Australia - responsibility for security.

ealthier mindset

| ITSA & ASA training courses (Cross govt) | APSC - led.
- how to think like ITSA
- templates to use | avoid challenges from eco's at scale.
- risk assessments to copy off.

s 33(a)(i)

[redacted]

Document 1

• ITSA & APSC training
/ evaluating training
onboarding: / integ^n with PMC systems
• tailored to levels of staff.
• Poli re clearances & breaches on staff.

Emma s22 [redacted] (HR).

Anecdot: s 33(a)(i) [redacted] different understanding of security.
s 33(a)(i) [redacted]

Physical loc^n - set up very differently in terms of managing material.
cf Tsy (breach) culture.

'Here' - more relaxed.
Barton - depending on which bus area ⇒ diff cultures,
- expect^n of Cab Div that outside Cab Div is good.

Highly Mobile - @ leadership level as well. | Re 'risk'.
(turnover stats)
↓
No.s for SES but no reporting f^n as yet.

• Secondees affects culture, dilute culture with diff preferences & ways of staff coming in.

Traning
- Does HR run all training for dept? Particular areas lead?

s22 [redacted]: have e-learning Modules (bus areas come up with content)
- we provide access via Learnhub.
- no face to face via HR.

Don't evaluate. Don't have capacity to evaluate.

Pick up generic modules ; APS wide.

PMC 'purchases' Dept of Educ^ system & modules.

HR provides platform ; areas provide the content.

↓

either other depts or private provider to get access to Modules.

e-modules : cost effective to run ; easy to update.

Ric - elearning ex of IT ; no additional breaches ↓ in moving to e-learning.

Q^ whether compliance (via elearning) is right approach &

- targeted training around risks in dept but how do you deal with a fluid staff environment.

No single entity in Corp has no clear line of sight to staff entry levels. | disconnected systems. |

Discuss^ re automation (including outside corp)

- no-one pushing first domino & domains don't align.

Ric - Recalcitrant (breach) offenders

- from Wellbeing team via Security.

⇒ investigate.

Security f^ can withdraw security.

HR f^ - talks to managers in area on options & assess risks

[redacted]

Doesn't fit in HR space.

- Removed staff via misc. leave ⇒ then took action

- Relatively informal convers^n.

- HR : take legal advice.

Rec - come up often?
  2 in last few months. But generally, not often.

Are HR thresholds the same as line areas?
  - yes:
  - not always with line areas ; can be within corp if don't have say IT data
  - never remove access / remove other w/o evidence.
  (Under Fair Work Act - oblig^n for staff)

Security waivers?
  - formal process (in other org^n) ; deleg^n with Dep Sec.
  - HR role light touch ; ensure process takes place to get in door.
  - PM&C different , PM&C 'that person' : generally less risk.
    : judgement balance

s 33(a)(i)

[redacted]

s 33(a)(i)

* Revisit learning with Pat.

WP - HR not consulted on Dem Srvce process & establishing common footprint, which includes learning modules.

Wish list
- to be more coordinated; coherency.
- Charlie picked up all Corp f^; bring all elements (w corporate) together.

Rec reshaped that role w/ ASD CoP is attended by Alan but thinking it should be under Steph.

Emma - having someone not w Governance but Champions security; external champion - not pushing own agenda; someone from outside Corporate.

q^ - more prominent role for Alan rather than move to Stephanie?

s22 – Tsy

?ic - not share lessons learned

s22 - offered up

?s - tempted to say reports be shared

Tsy - didn't hide, informed other agencies

- AFP didn't want to be involved.

- Shared review with every agency with whom we gone & share recs

s 33(a)(i)

facilities within CFO. but ASD ITSA not part of facilities?

See Tsy structure – ↑ separation of responsibilities (see later)

s22 - ASA underneath & ITSA underneath him

⇒ Chief Security officer (only new)

Recom - Band 1 position

Security needs 'seat @ table' : FIRB, etc.

In past, APSb / ELI's get shoved aside. (Security = impediment)

CSO ≡ cust. service.

= soon as say no; officers find workaround

Shows value to organ".

Require Band 3 via deleg under PSPF.

(why s22 reports to SES 3)

Public^ or pert. in Ann. Reports?

Document Training
[redacted] ⇒ link to APSC, wider network?

- Security training mandatory every 12 months; face to face; 1 hr (30 min IT, 30 min Physical)
- ASA & ITSA both go.
- Secondees get 4 weeks to attend.
- Training once every 2 yrs
- SES 3 support : breach @ any level informed.
  ; Tsy security ; support of Exec & resources.

- people don't ask q^ of e-learning package. "Survey" - keep clicking.
- face to face enables ASA & ITSA to also identify any issues 'on the ground'.

- PSPF * vs prescriptive ; have pendulum back?
  - ASA & ITSA - still rev b'cos PSPF is new.
  - ↓
    ASA 'little educ^' ; positions difficult to make redundant.

- Org^ can pick & choose under PSPF.

Ric. - AGD ; no sense of security hygiene across APS; best practice?

A - PSPF mand. reporting = joke.
One agency reported full compliance 36-36 when located under Tsy pf and Tsy itself not fully compliant.

Team = 14 (of 700/800 in Tsy proper)

- Difficult to find a good ASA with support of Exec.
  - balance bet^ confidence of Board & arrogance of individuals.

Closed ASA school last year - check Patrie name.
- AG's had causes but closed.
- fantastic research.

[redacted]

[redacted]

- facilities - getting job done. But security in charge of facilities ⇒ aggrats - diff requirements they are trying to achieve. Also compete for funding.

Rec's - implement all? (Yes).
- How implement?

s22 [redacted] Sec laid down law; rec's implemented.

- How much was written to security policy? All of it, & more.

s 33(a)(i) [redacted]

s 33(a)(i) [redacted]

s 33(a)(i) [redacted]

- weekly snapshot to Exec
: breaches, movement, clearances. Communicate to Exec which is then pushed down.

PMAC lacks the incident culture of how breaches are reported to the Exec.

s 33(a)(i) [redacted]

Honesty system - staff not precluded if incorrectly file something, or call security @ 11pm to note container open.

No more than 2 people can access 1 container.

↓

PMDC has 'Gallagher' system - exists that connects PMDC corp system.

R.c. No breaches in year?

s22 241 in calendar year. (40% red in year previous).

Security snapshot - every 2 week.

Prod'y vs security tradeoff.

- surged vetters to cope.
- " on comms; seconded Comms from Defence.
- most people in TSy don't know; strong customer focus to ensure prod'y not affected.

s 33(a)(i) [redacted]

Even most simplistic guides not read

⇒ why training so important

Open-door security policy ; monthly standups (ASA / ITSA get 10 min slot).

Comes back to customer service.

12 months to Δ organ.

- everyone trained from Sec down (in 3 months?).

Rec - ASIO helpful.

s22 Yes

- embedded in FIRB Board.
- customer rel^ person from ASIO once per week.
- help to monitor staff ; mandarin expert to review corro.

Rec - physical security?

s22 - No.

Rec - mand. requirements, suggestions

No gov't forum that can invite CSO, ITSA, ASA to upcoming ASA & ITSA's.

- Gov decks : difficult to find ASA's across Dept.

- ASA's : formal test to weed out redundant / incapetent ASA's.

Rec - ask Pickles to certify opened & empty?

s22

- All bids fairly robust
- remove ~~pull out~~ bottom drawer to deck cabinet.
- Tsy goto scrap metal agent. No different in cost / return to disposing under guidelines (renovations, ~~etc~~ management fees, etc)

Worse case scenario - drill lock & remove bottom drawer.

[redacted]

[redacted]

WP - if not AG re security incidents ; who?

s22 [redacted] - not sure. They almost work indepen. No WofG one-stop shop.

They will share all security procedures - way to link Cornwell report to PMC actions.

-

public ; not classified. Willing to share because its public money.

back down via s22 [redacted]

* Value created will ensure support beyond current Secdray.

Discuss on tomorrows ToR 1 : what are we going to say.

as Account authority? — • Challenges to resourcing.
• Chief Risk Officer?

Charlotte

• Pushing own issues in Exec Board.

• Difference – use to be two SES 2. (Deb Lewis Head of Corp.)
bottline to do EA; asked to take on

• Issues symptomatic of Corp issues.

Complicated – different layers of security (Cabinet, NSC, satellite assets, etc.)

CT – many of MoG'd staff still on non-class. system.

PMC's Protective Security Plan is outdated.

Charlotte – no's on staff. | Note chat with s22 [redacted]
→ best from Corp or HR?

* Ric's point re language – need to professional editor.
– Ric likes 5 page FAQ with hyperlinks
– point: not everyone needs to know: it's not one PM&C in these matters.

Visibility of Exec Board of Sec. matters?

– CT: lack of reporting of corp hygiene
Asked to consider what could be reported.

Ops committee: policies in place; ie. physical infrastructure to meet the PSPF; not compliance & hygeine

Deliberate dec[n] to end routine checking of clean desk policy. (Sec X)
⇒ tolerance & behaviours undermined

RS – overall, need to harden up culture

CT - It's a different 'posture'.
- need reminders as don't have complacency!

RS - IT more public than protective security.
- better networked

CT - In security; end up with unplaced people.
⇒ Security team w/o expertise (also property)

RS - Facilities & protective security: lessons having in same branch.
- Also phy strong role in IT
but Also not so strong in Asm & phy security.

Data - RS asked CT for.
- No incidents & types; breaches by Div^
- what do with breaches
- clearing levels: pre & post MoG.

- Barry replaces Alistair; but not clear of overlaps.
⇒ enterprise role (which is separate from CFO role).

Ric - arrange meetings with Barry & Lin.

Emma - data on staff mobility.

[redacted]

[redacted]

Op Committee (monthly meeting)

- in process of transferring from Brenden Jarratt to Charlotte.

s22 (working with Will Stacy a Charlotte).

Govt Security Committee - is this a COP?

(See Alice)

Does Alan go to this?

Methodology

s22

- Payroll

-

PAT & s22 [redacted]

Cap. governance.
-Sense of interest from EB.

PS - Not to EB, but yes to Ops Comm.
↓
Under Review: looking to balance strategic & operⁿ.
-Security reports 1st year
plus 1 to present PSPF report | Operⁿ Committee
↓
once advised ⇒ to ~~Martin~~ Martin to sign off
& write to PM

Dep Sec. Governance - historically not a strong role.
Eliz Kelly - looked @ Security Roadmap.

PS - on day to day ⇒ More about expediting security clearances

Risc - Traffic light system?

s22 [redacted] - not by Divⁿ or Fⁿ.

Barry's role: Chief Risk Officer
-Alistair had prev. role. ⇒ departure; role to Barry.
More strategic; enterprise risk rather than 'nuts & bolts'.

Operationally: risk assessment basis

(Risc - culture flows from top.)

Staff – line diagram coming from s22 [redacted]
⇒ getting new version.

Ric – enough time?

PS – q° turnover, qualified people

Focus on PSPF non-compliance & security clearances (ie G20) → Δ u PMO
⇒ housekeeping like safes register falls aside.

s 33(a)(i) [redacted]

Nb's view: need short-term ↑ to pick up on housekeeping. (*)

Ric – on data
: Sec. clearances; rate @ which get them; outstanding.
+ breaches

in culture box ← impact on security culture & environment

Ric – is data we have good enough?

s 33(a)(i) [redacted]

Stats received

- MoG 2013: light approach to ramping up patrols @ LAG.
  2015 "One PM&C" approach ∴ incidents increased

PS - what to say about data? | WP apple PS + s22 [redacted] on process for building pass tracking & reporting.

Training

• e-learning + PS @ mercy of small LAD team.
  - have to ~~fo~~ compete for priority for training with other areas

• Do we have a 'training person'? (No).

s22 [redacted] - Physical Sec. team provide bulk of content

PS - Try example; fortnightly training but everyone @ least once a year.

PS - 'had' a system like that (CASA + TSA)
⇒ moved to e-learning.
No desire to enforce 'mand.' training.
Up to business areas to direct staff but e-learning process doesn't allow to track who hasn't attended training.

Everyone - annual refresher - online.

Face to face - on request: grads, taskforces. Look to over page.
Due udep. risk assessments on areas.

PS - induction is a broader problem

s22 [redacted] & No consequence for non-compliance.

[redacted]

q° of regionals & unclass'd info & protect'd network.

Rec ; [redacted] Offices w National offices (one Nat Circuit & weekend) attend face to face once per year. (Settle on some approp. words.)

AGD CoP - to gain new policy.

s22 [redacted] AGD process ropped up & informal CoP of ASA has dropped off.

s22 [redacted] Tony - host ASA CoP ; informal (ASA & Assistant ASAs) | within Prot triangle

Project upgrades w next 2 years; everyone must do (Type IA alarms).

RS - AGD : more helpful role w this space?

Sense of hygiene across APS? s22 [redacted] - no.

RS - formal role? (Not people doing PSPF guidance.)

PS - q° of role @ next level down for housekeeping?

⇒ Central agency provides to portfolios & many dept distributes to portfolio agencies.

PS - cross agency info is an interesting space.

- Induction process : people w to APS

- good @ grades plus SES

but people w but ; not good.

⇒ no real requirement / mandatory induction

s 33(a)(i) [redacted]

PMAC roadmap - done late 2015. s22 'living document' which will be
Same with Security Strategy updated.

Protective Security Plan - being updated by s22 team.

[Check s22 online process.]
- getting that support would not have happened w/o the incident!
- Same with Servicenow.

(Deb)

Corp Services + Finance Services

Bus. Info People Fin % Budget & reporting

Deb to EA.

End last year: Corp Div^ - all 5 under Charlotte (excluding People).

* PS - Works well under Charlotte.
- Value for Nathan & Pat => reporting to CFO useful.

Principles vs compliance

ie. make the rules clear.

updated security plan ; now reference to safes.

(But PSPF = principles-based doesn't reference safes.)

Go to Caroline - how?

Awareness - great but practice is poor. (Why disconnect)

Don't make individuals responsible.

RO - distinguish betn NSD & Cabinet (ie in terms of importance of docs)

s 33(a)(i)

s22 decentralise team. Located one officer in Cab Div^n?

12 Major regional offices - s22 (?) in Woden ; establishes Security Champion in each site

- fire warden ; first aid = each get $50.

Alternatively : est. Champion within teams.

(est Wardens in teams).

Security is everyone's responsibility

Moving forward ⇒ more to digital environments

MEETING WITH s22 [redacted]

Single secretariat – for EB & Operations branch, & people.
– F^n from WIL, GAES & people branch.
– finalising recs for Governance review.

| Audit Committee separate.

Monthly meeting – on how PM&C is running.
to EB. – what needs to do.

Charlotte – operations report to EB.
– dashboard with who need to see. Seen by ops & ⇒ flag issues to EB 4 (decⁿ – more active). Not FYI for EB
– covers finance, IT
∴ Could add in security reporting.

Q^n: do use internal audit process to
– Audit Committee ~~to EB~~ work programme to EB. Get EB to sign off on work programme for Audit Committee.

– Audit Com has budget (might be more feasible that s22 [redacted] & Pat doing independently within teams). needs quarterly.

Op^n role in Audit – monitoring response to recs.

Ops – Andrew & Stephanie (co-chair)
– Tony & David G.
– Barry actively involved.

| re-jig (SES1 & 2's from each group)

Corp SES – as advisers but not on Committee.

Once a month – 5-7 days out from EB

EB meets monthly (monthly for Ops).

EB: All Dep Secs plus Martin.

Enabling Services
⇒ Corporate Master data project.

Pat - get detail

Sam Volker - Tableau (software licences)

↓

enable data to be pulled from the one whole-of-PMC database.

Next EB - 26 March

EB - 13th March.

EB - 5th March. → Verbal discussion.

↓ check with Ric s22 chatting with s22

Service Now ⇒ not a sol^n in itself.

⇒ Making from : not responsive to Security risks & needs.

⇒ need a responsive security to breach

[redacted]

MEETING WITH DEB LEWIS

- Security culture @ VAG
- Transition from Corp to Policy area
  - For SES staff: what sort of induction (reduction) did they receive.
- VAG: security support via ONE?
- Deb's reflections on past EB engagement & current Corp restructure.
- Reflections on WYW - any discernible behavioural Δ's?
  - awareness training for staff?

VAG work closely with Cab. Div^.

s 33(a)(i) [redacted]

- Need 'online' would be good (re. training)
  - what

s 33(a)(i) [redacted]

Different level of familiarity (with cab processes)

- Deb: not as well versed with digital documents, working documents, secure^ Would be useful.
  - eg One note beneficial but mindfulness in terms of what you are recording.

[redacted]

- 30% turnover plus private sector.

In past 2 its IT style to work with Board.

EB – 'disinterest'; lack of engagement by EB or how organ functions
Charlotte's presence – because of finance updates.

No engagement from AGD.

Vulnerability around devices
CDP – printed copy; not everyone paper like.

International work: IT support – first time – yes
second time – no.
– other staff: indifferent if received training.

Deb – sore when travelling on holidays.

E-learning – ok as long as short
Face to face – real life scenarios.

Anne Marie – regional managers to Canb 4 times a year.
=> incorporate security as part of those catch ups.

Issue of digital understanding coming up

s 33(a)(i)

[redacted]

[redacted]

Induction - for grads yes but no-one else
- should be mandatory face-to-face.

Yearly on-line = must.

Q^ ; ELI A above ; face to face.

Δ in security - reaction (ranked understandable)
⇒ but can't go around breaching in absence of causes^
in climate Δ ⇒ start @ top.
Run @ next SES.

⇒ SES talk to staff.

People curious, but not sure how to use digital devices.

* The reoccuring theme around staff & their understanding of how to work securely in a digital space and file with the profile of people wanting to do the right thing but not knowing how. ⇒ can lead to good behaviours (with the right coaching) & bad behaviours if staff pass on the wrong knowledge.

Archives, RoSmith. 7/3/18

* HPP investigation ongoing, not connected
+ review timely, digitising, HBW, update policy
+ complex environment, spectrum of activity, mosaic
+ close to finishing draft.

* DF – interest in integrity of archival resources
– records of Cabinet, keeping integrity of record
– HBC covered by Archives Act, letter to PM&C/HPP
– unauthorised transfer of records? ☐ HPP
– recognition of obligations under Archives Act.
– contribution to make? equity in incident.
TW – contact with Cab Div – Heb – Michele Graham
– regulatory powers over Ch agencies
DF – integrity of archival records
– release decision – public knowledge

Cabinet Division advice ☐

– breach of Archives Act – HPP consideration? ☐
– HBC legislation?
–

RS + disposal
+ need for HGD guidance
+ document management – tracking records
DF + Archives Act responsibilities – incl. IT.
+ information governance / management standards.
+ part of corporate governance.

DF + recovery records
+ alteration / adding / subtracting.

RS + also looking at culture & practices

DF + resources – best thing to do is easiest.
+ consultation – RMO?

15/2

Mtg with Pat & s22

- Pat to try & review 'interlinked' TORs
- Ric no role in investigation
- Complex working environment
- Responsible for WoG Cabinet material
- Lots of TF, secondees etc
\+ - Data from HR on internal movements
- MoG implications from 3 years ago, 800 to 2500 very quickly.
- Tempo of enabling services (re TFs) has consistently been approved.
- Updated
- PM&C rates highly on PSPF self assessment scorecard. Doesn't assess behaviours.
- ANAO looked at 2015
- Ops Committee reviews. Stephanie chairs.
- Security reports 3 times a year.
- Considering compliance incidents, dashboard
- Working your way) how did we address security risks in considering)
- High security areas excluded in Business case
- Fiscal & Cabinet worked closely on design
- International Safin High requirement
- Rationalisation of resources
- WYW opportunity to improve behaviours.
✓ - Centraplaza tour
- Paper based dominates in some areas. zoned, electronic & ~~paper~~ paper based

- What additional guidance is provided to staff on security for WYW
- Records mgt working with areas → digitising records
- ① Opportunity from crisis ② Transition to WYW } behaviour/culture

① - move from excuses to accountability
② - education, induction, aftercare practices for high security

- Reasonable on s22 [redacted]
- Records & Info mgt presentation (Natalie)
  → Get for Ric
- Investment in IT?
- Hard to trade
- When incidents occur } do you get notified (Martin)
- PM&C started ASA
- what extent does AGD manage the community.
- s22 [redacted] L&D } s22 [redacted]
- Who are others } Kylie Bryant
  Lee Walton / Chris s22 [redacted]
  Trevor Jones
  Allan & Tony
  s22 [redacted]
  Gov Div

- Consequences of not doing training } money
- Meet again

Mtg w Yael

Snapshot of Division
FOI > Gov Div
One person looks at it, up to an SCS
Document mgt
Protocols in place for mgt of information
Gov Div holds FOI material,

FOI request (obtain sample for Ric)

Cab Div doesn't keep paper copies)
electronic filing system.

- We have a safe / they have the space. To store IB docs
- keep docs for the Term of Gov
- Work our way
  - mandatory requirements
    - secure area zone 4
    - zone 5 for NSC
    - compactus (4+5) B) B class
    - access to secure storage, reading areas,
- What is the induction
  - ⇒ have a pack
  - ⇒ note taking, parts depending on role
  - ⇒ Cabinet specific

- more train on handly official records what to do with your work documents after you've finished.

- exit points > procedures & processes.

- Cab Div doing own audit of safes. Bi-annu

- key safes > corrupted

- SES to approve removal of safes in Cab

(1) less reliance on paper

(2) Digital security > - do people know how to do this properly
- how do FOI people/lead at digital

classif

(3)

=> work place hygeiy
=> y

=> Mgt of safes ; &
=> Mgt of documents

15/2

Mtg w AGD
Sarah, Anna, s22

- AGs role: retained PSPF Attorney responsibility
- 36 to 12 (streamline)
- focus on cultural
- PSM to PSPF in 2010. More principles bas
- Information security Manual) lots of rules
- Lack of clarity) lots of material, confusion over mandatory, too many rules
- Back to First Principles
- Risk based decision maki) agency level
- Refer presentation
- Government Security Committee) Dep Sec Chaired, AGD

#⇒ Stephanie Forster) should she be rep instead of HR
- TS, Secret, Protected, FOUO

- learnings from reviews not done at the moment.
- Government Security Committee could discuss if shared.
- Best Practice Dept) impacted by MoGs
- ANAO) currently focussed on personnel.

> Parliament House - does the PSPF apply.
Yes, agencies support office, but so does parliamentary

> AuD doesn't audit

> Forum to share experiences

> seller & buyer have responsibility

> Accountability > is there enough 'joy' around document hygiene

---

Myra Ric

⇒ modular learning vs face to face
⇒ mo impacts
⇒ unhelpful documents

⇒ Box's in report of PFCP, what we did. Our compliance report

⇒ Meet with Allan, Kylie & Chris A

⇒ re-do recommendation 4 TOR

⇒ Interim by 9 March (latest).
⇒ Wayne's email

- handling of info & accessible
- movement of safes
-

⇒ Principles to compliance

AM> Work your way is not conducive with NSIP work
> Confident of NSIP Group security capability
> Grad analogy
> Bagged, accounted for handled properly
> Disclosed of briefer
> Absence
> Consequences to poor security hygiene
> ~~high standards~~ & pa
> intelligence packs tightly held
> went to zone 4/5, caused ramping up of security arrangements
> Zone 5 can't have laptops
> Lots of discussions on work your way to apply lessons but make Zone 4
> allows downgrading of clearance
> clarity of information / bins are confusing
* Can you put Prot-Secs-Cabinets

> There's nothing around Cab exit document on safe mgt

> locally staff now told not to inherent content. You need to leave & ask arrange transfer of

> security said we need CDR's for safes? Unworkable.

> Need policy before we develop measures.

> Everyone got prompted recently to do mandatory security train.

> Not major hadley > down in the weeds

> complex issues, lots of protocols. Simple issues in the absence of documents

> Minimize what you keep, pragmatic about disposal.

> AM > worried about CDR complex issues.

> Names need to be allocated & responsible for documents given to individuals.

Behaviour

> Lessons learned > disciplinary action

> Buddy systems, comms messaging

+ People Mtg wk

- Exec Board / Ops Committee > Secretariat Kass
- As per governance, review
- Monthly meeting > how does this place run. Exec Board. CFE developing report. Dashb Ops considers then to Boar for action.
- Can we see Charlotte's report?
- Ops monthly report on state of kasi
  ⇒
- Shald we use internal audit commit to monitor implementation.
  → Band 2 level (in brnale exter
- audit committee has a budget, health
- Audit sets risk, Ops manages
- Ops Comm > Andrew, Steph, David, Barry (risk officer), Band Group representation
- Corporate ses advisors as required.
- Colm from NSIP
- Ops monthly
- Audit quarterly
- EB weekly + monthly governance
  ⇒ action decision mak

EB + Martin and Dep Secs

Dashboard ⟨ HR content

CIO report monthly to OPS

Corporate Master data project → project to unify data identifiers across multiple systems > Pat Sonny!! — 18 month

Governance
Procedures
Behaviours

* s22 to provide words on transformation

Sam Volker > TABLEAU Reporting tool.

EB on 26th - release publicly

→ 13th

→ EB on 5th?

Mgt w Sarah C

AgD — both ICT + Personnel/Phys sec presented together

Data gathering is challenging

AgD — classification noted in breach

Security Champions) similar to ours

(1) Spectrum of risk - ranges espionage, insider threat, cyber attack, physical risks

Core things in PSPF,

(2) AgD role ⇒ drivers of PSPF

Chairs Government Security Committee (quarterly) ⇒ sarah chairs recommend DpSec Governance be person

Community of Practice (multiple)
Who attends) EL2 level / EL1
- digital footprint etc
⇒ Does PM+C participate? Anna to advise.

- At end of Sara's meeting classified meeting chaired by ASIO (check Allan's role).

- Community of Practice > Knowledge incidents to be shared at junior level and push up to strategic level

- Potential for AGD to take on a greater role?
  Yes.

- AGD have would like to have better visibility of major incidents
  ⇒ develop a way to share
- Transparent environment (re Fraud example)
- Could AGD impose a requirement to report significant incidents

- what if PM wanted reports.

- AGD change reports to provide a more comprehensive picture. But they don't have incoming picture across you?
- Resourcing > an issue for AGD.

Quantitative vs Qualitative

- Is there an appetite

⇒ Reporting on incidents, and actions taken since. Needs guidance on threshold.

⇒ Ric to share with Sarah & Anna. Maybe speak with Chris.

⇒ Training > Protective Security Training Centre closed. Gov decision not to be a provider. How do we engage with providers?

⇒ APS wide governance > implications > good framework.

⇒ Encourage users to use training course

⇒ Sold for scrap > instead of ex-Gov > AGD. Locks removed before selling on.

words on AGD

PROTECTIVE

Cyber > Physical & Personnel Security

513

Mtg w Pat, s22 Nathan + s22

- ITSA + ASA
- Chief Information security officer > Nathan — CIGO, CIO, CYZO
- Cab Div > additional layer of protection?
- Cab Div report > results of Musters. Talk to Paul
- Internal audit > cycles thru all areas.

→ Data specific & 25 to relevant to phish.

s22

- CIO report 'monthly' Quantitative rather than Qualitative Ops → Audit. Bi-annual to Expert Board.
- Incident reporting goes back 8 years

Harder in the personnel & physical security space. Standardization of Guards required.

CZ east > 3 agencies / Trevor HA Bo
CCTC
ONA/I

→ transfer of documents, ICT connec

ITINERANT

Can Security assemble data to repo

→ Taskforce > deliver mentality

If [redacted] identifies incident, [redacted] team

Database > 4 different areas / fraud physical / +IR ICT

↳ being built.

- Board would appreciate single report

- Resourcing / Training Re-work manual

.1 to .2 FTE Pat [redacted]

15% documentation

15-20% stakeholder engagement

20% complex vetting clearance

→ 15 people FTE < 10 part ~~time~~ pure
3 people
2 parl

> Guarding contracts up in June)

ITSA & ASA do overseas travel briefs together with ASIO

ASA > COP info tool to rather than useful discussion.

- AGD to provide professional pathway or advice for security professionals.

↓ quick assessment of where the training is.

⇒ APSC & AGD could work to return to design something similar to the APSC/digital dataset.

⇒ Accreditation available in RTOs

⇒ Gap in vocational security training ✗ We need to get interface of physical & ICT security. Needs to be in the early forward.

- DSS looks after ICT for regional networks.

- Sites that have protected, regional office.

- Can you go to cloud? re Andrew Jay Business case under review Driver: set out of DSS Organisat needs to pivot regularly

→ Threshold of incidents

Mtg w Trevor

- Procedures fairly good
- Cultural issue > human behavior
- NSIP good procedures)
- Mgt of paper documentation, generational.
- FOI?
- Digitise TS docs > resource ?
- Over classify docs > can we de-class documents down the track?
- Culture / Accountability
- Sample > audit, spotcheck
- Sticker on top signed by ASA
- Can we archive stuff we don't need in the TS space. Re electronic archive.
- Bins are confus. > signage. / random audits
- No decommissioning of TFs.

We need a line in their about need to know vs consultation. Changing dynamic of Cab Docs.

new level of 8/9 … right with Mr Warrie

6/3

s22 [redacted]) the Australian

Mind a changing

Growth in Committee Cabinet

- 2003 strong paper based environment
- Less national security based
- Cab Docs held in elevation Increased
- consultation has changed dynamic
- CabNet viewer + do too many people have visibility?
- We need to find a better balance of who 'really needs to know'. Perhaps gone too far??
- eroded principle of 'need to know'
- NSC, Cabinet & other Committees expanded & volume
- Cabinet Div mixe of staff. Some quite new ~~[illegible]~~ Refresher & reminder of principles
- Ministerial offices) need a strong security culture. Micro pink slip
- Pressure on DCO, to ensure there aren't → Workarounds in Minister's Offices.
- BC need to be tinkered
-

Security Champions

(1) Format
(2) The issues! (3)
language related to particular … [illegible]