Australia's Cyber-Security Strategy 2016 & 2020.

Comments from Chris Drake, B.App-Sci.

Email: cryptophoto@gmail.com
Phone: 0487 543210

About Chris

Foreword: Australians suffer a cultural affliction known as "tall poppy syndrome". It is in our nature to despise, criticize, cut-down, and distrust high-achievers and public figures. Please be aware that you're in Australia, and probably you are Australian, and are yourself almost certainly so afflicted. If, while reading this, you find yourself critical of my motives, hating my words, or thinking anything about "Chris Drake" – please STOP – take a breath, and try to return to the topic. This is about Cyber-Security – not about "Chris Drake". If you're thinking I'm arrogant already – perhaps take a break right now! Disrupting "tall poppy" is an important step to securing Australia!

- I'm a veteran cyber expert with 37+ year's continuous experience, a vendor, and I'm trying to fix Aus Govt cyber.
- I'm a graduate from the **excellent** Israeli Landing-Pad Program by Austrade.
- I'm a Microsoft-Ventures cyber graduate (India) and an Advance.org cyber graduate (San Francisco)
- My cyber-security company has raised more than $1M through several federal Government grants.
- I was on the PM's cyber panel. I've been part of two cyber advisory committees (e.g. network threat blocking).
- I've participated in 3 senate inquiries relating to cyber.
- I've been involved in numerous QLD state-Government innovation initiatives, attended many QLD events,
- I've made use on more than 100 occasions of cyber vulnerability reporting mechanisms throughout Australia.
- I've personally met ASD staff several times, and attended private lectures they've given.
- I've made extensive use of FoI-Act requests relating to cyber security issues, and filed one Privacy-Breach notice.
- I've reported more than 3 critical government vulnerabilities in the last few years.
- I've worked with the AFP and FBI for many years, and testified in Cleveland putting BayRob in jail for 37 years.
- I wrote the penetration-testing guide of our Trusted-Digital-Identity-Framework, TDIF (under contract to DTA).
- I'm a vocal AIIA member in cyber advocacy groups, and regular attendee at cyber forums and events.
- My company and I have won more than a dozen prestigious international awards relating to cyber security.
- I own many patents, including the worlds #1-cited security patent of all time (authentication & anti-malware)
- I've worked in Anti-Virus research at IBM. I'm in the partner programs of Microsoft, Checkpoint, IBM, and others.
- I've personally hand-coded 3 cipher algorithms under contract to the Australian Air Force.
- I've taken one of my products through the ASD (formerly DSD at the time) cyber evaluation process.
- I am a USA-accredited digital identity registrar and run a secure online identity service
- I'm an AUSTRAC-registered digital currency exchange, participated in their training, and got audited
- I helped write the OpenID, OWASP, and FIDO standards, and some of the NIST sp800 series.
- I've submitted several cyber-bugs to international bounty programs and reporting systems.
- I've had meetings of 1+ hours each with more than 500 cyber experts in 200+ different global organisations.
- I'm a member of a dozen cyber working groups. I've won several state and national GovHack awards.
- I've spoken at about 50 local and international cyber events, and attended many more.
- I've sued and successfully defended cyber patent and trademark lawsuits in the USA
- I own and operate an Australian cyber business in the field of secure authentication.
- Cyber-security in Australia is a shambles, and I genuinely want to try and help fix it.

Most of what follows is not my opinion – it is fact which I can support with extensive evidence.

There is no substitute for experience. Anyone who hasn't lodged a vulnerability report, participated in an inquiry, filed an FoI, used a cyber service, joined a cyber group, built a standard, been at a working group, sold a cyber product, run a cyber business, tested an assumption, etc – is not truly qualified to comment on the related topic.

Proposed call agenda, Thursday, October 3·2:00 – 2:45pm

Participants:-

- Chris Drake
- The Director of the Cyber Security Strategy
- and Governance team?
- Home Affairs representative?

Introduction:-

1. Tall-poppy problems.
2. About Chris Drake.
3. About each call participant.
4. Discovery of the roles each participant plays in production of the 2020 strategy. Who else (not present) drafts it? Is it already written?
5. Topic familiarity survey.

Discussion:-

1. My written response (this) – it's too long to cover on the call…
2. My recommendations (so we don't run out of time before getting to them!)
3. Detailed discussion of the strategy topics (my annotated views paper)
4. My offer to help: I propose I lead an industry team to help draft the next policy – The government should not write this strategy alone, and the strategy itself says industry collaboration is "increasingly important" and claims that ensuring our online interests are protected requires government and industry "working together". Prove this is more than rhetoric. Work with us to draft the 2020 strategy.
5. Possible further exploration of this topic (I'm happy to talk more, to delve into any specific failures, to supply evidence and "name names").

Comments – 2020 "Call for Views".

Recommendations from Chris Drake

Government's role in a changing world;

1. Stop undermining our industry – I manufacture **extremely effective** cyber products, and the following defeatist attitudes and outdated, unhelpful, mostly-wrong statements are making my sales efforts unnecessarily hard, are preventing uptake of solutions, providing justification for failures and for not trying to fix problems, and giving everyone the wrong mindset:
   "we can never be totally cyber secure" (page 14)
   "Australia's 2020 Cyber Security Strategy cannot be a magic bullet" (page 20)
   "A new Cyber Security Strategy … would be unrealistic to expect it to solve all problems" (page 20)
   Get rid of all those statements please, and stop issuing any and all related defeatist language. The "ASD's Stay Smart Online program", and tons of other advice, is similarly riddled with this same language and attitudes.
   STOP TELLING OUR MARKET THAT OUR PRODUCTS DO NOT EXIST OR DO NOT WORK!!!
2. Stop Blaming the Victim – Every time you say any of the following, you are blaming the victims. You are educating the only people who can genuinely keep them safe (their providers), that it should not be the role of the provider to keep them safe. Things like:
   "Cyber security has always been a shared responsibility" (p.8) or
   "raise national awareness of online threats" (p-5) or

"Australians need the right knowledge to make cyber-smart consumer choices" (p.16) or
"we need to know how to be more consistent in practicing secure online behaviours" (p.16) or
"increased consumer focus on cyber security" (p.17) or
"Our hope is for all Australians to play a role" (p.18) or
Almost the entirety of the "ASD's Stay Smart Online program" (p.32), or
"behaviour change initiatives" or "user awareness" (p.16) and worst of all
"Australians continue to fall victim because they fail to observe, or are unaware of, basic online security practices" (p.7) – this is **BLATANTLY UNTRUE** – they become victims, because their providers have not given them solutions that mitigate the everyday problems of human behaviour.
Stop doing/saying all the above. It should NOT be the job of 25 million Australians to all be cyber experts. It SHOULD be the job of companies that provide services TO Australians to comply with and offer sensible cyber-security protections, so that those users are SAFE even when they are not cyber experts.

3. Educate industry, institutions, and government that THEY should be responsible for keeping their users safe, that THEY should deploy suitable protection for users, and that everyone should stop blaming the victims.
4. Your first paragraph says "we need to adapt our approach" after acknowledging that things are getting worse. The concept of "Innovation" requires discarding practices that don't work, and embracing new solutions. Take your own advice – re-read my #2 and #3 recommendations and put them in place!
5. Combine all the dozen-or-more threat-reporting bodies into one. Fun game: who can name the most!
6. Discontinue all location-based cyber activities: Australia is far too vast to expect everyone to go somewhere for meetings etc, and online systems for this purpose are already excellent.
7. Discontinue collecting "do nothing" victim statements – *Every time* a victim contacts you, DO SOMETHING **IMMEDIATELY** ABOUT PREVENTING MORE VICTIMS, and where possible, help the victim.
8. Ban the public sector from building their own cyber-security products and services. I do not appreciate my own tax dollars being spent hiring expensive contractors and more public servants who build things that directly compete against me, and which cost 10 to 1000 times more to make than if they had just bought mine in the first place! What they build almost always fails, usually at spectacular expense, is never properly secure, is never commercialised, is usually duplicitous, and is robbing Industry of jobs, income, adoption, commercialisation opportunities, and robbing the Australian Public of quality secure services, and online protection.
9. Discontinue the suppression of senate-inquiry submission records.
10. Discontinue all suppression of public submissions relating to cyber security – if confidential material needs to be suppressed, there should be a formal review process and censorship using "blacking out", instead of a total cover-up of submissions.
11. Extend mandatory intrusion reporting to all Government departments – the cover-ups are preventing remediation, and there is already no penalty for failure or non-compliance.
12. Amend consumer protection and competition laws to include Government – it is grossly unfair that industry has to compete against government in the first place, but when the Government does not have to abide by normal consumer rules, it's doubly unfair. For example – DTA marketplace price caps would be illegal if they weren't Government. "Clear and reasonable rules that protect consumers and keep risky businesses out of the market are good for everybody." (p.11) – this needs to apply equally to Government.
13. Hold business responsible for losses of their customers. eBay does nothing to take-down obvious scams. Telstra does nothing to prevent scam phone calls. Banks do everything in their power to shift losses to their victims. None of those businesses buy cyber protection for users, because they believe it's cheaper and easier to avoid/insure the losses – blatantly disregarding the costs this imposes on their victims.
14. Make cyber crime reporting by listed companies mandatory, including direct losses, insured losses, and customer losses, with large fines for non-compliance. E.g. Every bank in Australia has suffered large cyber losses. Zero annual reports of any banks list any of them.
15. Introduce minimum cyber security requirements for companies (and government departments) handling personal data of Australians, including AAL3-login offerings, TLS website security, telephone mutual

authentication, mandatory digital signing of applications, and so forth. The vast majority of all cyber crime is easily prevented, but companies/governments in a position to deploy prevention have no incentive to do so.

16. Fix government scrutiny and compliance. This statement: "Government's activity is also regulated strictly by law and subject to extensive external and independent scrutiny to protect the privacy of Australians" (page 9) needs serious examination: who said it? What makes them think this is true? Why is this in direct contradiction to every experience I've had? – If there really is any scrutiny at all, it's either wrong or being ignored (if you talk to the ASD, their #1 complaint is that departments ignore them).
17. Fix procurement. Australian cyber vendors should not have to find every department who needs their protection, and deal with the length sales and procurement process. Those departments should KNOW they need to secure themselves, and should actively seek out our solutions and buy them. The DTA marketplace is totally dysfunctional – the only thing departments can buy, are contractors to build new solutions that compete against industry!
18. Amend the ASD advice banning the use of "strong security" techniques for low and unclassified purposes; "strong" does NOT mean "slow" or "expensive" or "inconvenient" or "hard" etc – all advice discouraging "best practice" in all situations needs to be removed.
19. Comply with the ASM and all ASD Essential recommendations
20. HSTS, HPKP, and Expect-CT all be enabled for the entire gov.au TLD and all subdomains. There is NO EXCUSE for not using TLS in 2018 and beyond – these security technologies will force all departments to be secure, whether they like it or not (and, the bulk of government departments do not like it – but they should never be entitled to their misguided opinions when citizen identity/security is at risk).
21. Overhaul of the FoI act and practices should be be performed – there are too many exemptions allowing departments to cover up embarrassment, and there is no working review process.
22. All department ISTA roles should be made known to the public, that all ISTA roles be staffed, that all ISTA staff be properly qualified, that no unqualified persons be permitted to provide cyber advice, that all cyber advice provided be attributed, that ITSA staff be required to accept cyber-security and privacy reports and complaints directly from the public, and compelled to act on them within a reasonable and short timeframe, that all cyber reports be reported and made public, that no cyber reports be disregarded/hidden/ignored or otherwise not acted upon or reported.
23. Every department touching identity information should be required to undergo annual compliance auditing against all mandatory ISM controls, be fully compliant with all strategies to mitigate cyber security incidents (not just the top-4, or essential-8, but all of them. https://acsc.gov.au/infosec/mitigationstrategies.htm), that these audits be published, and that penalties be imposed for failure to comply.
24. No identity information should ever be shared with any department that does not have a current and fully-passed audit. Any reports to or by an ITSA providing evidence that any department is in breach of their security requirements should result in the immediate revocation of their compliance, and the immediate cessation of identity sharing.
25. That a non-government process or perhaps royal open commission with strong powers and penalty tools be undertaken to repair the near-total lack of cyber security response capability within government – my work is just the tip of the iceberg; a more thorough process needs to be undertaken to find all the other problems which are being covered up, and to repair them all.

Enterprise, innovation and cyber security;

1. It is imperative that providers do more to protect users. It's not difficult, nor expensive, but they just don't.
2. A purchaser is NEVER adequately equipped to protect themselves. The nature of most modern threats makes it an architectural impossibility for a user to protect themselves – the providers must offer the protection, because there's no other technical way to be properly secure.
3. Discard the "minimising upfront costs for industry" requirement. (p.12). We're allegedly losing $29bn annually because they're not securing us – them saving money at our vast public expense is not acceptable.
4. Cyber services should all offer AAL3 to users
5. Cyber goods should all be digitally signed

6. Companies failing to provide security updates (phone firmware, SIM card replacements, routers and modems, baby monitors, TV's and IoT devices, etc) should be charged a fine, and that fine spent on updating or replacing the insecure products. We passed a law letting Australia force anyone globally to reduce their security and insert back doors– why not pass another law forcing them to fix security problems too?
7. Private industry, not government, should be tasked with the broadest possible set of roles and functions for identity. Government is un-trustable, unaccountable, beyond reach of laws and penalties, and has repeatedly proven incapable of implementing even the most basic of security protections for identity information. Government are far more capable of compelling private industry to comply with laws and have penalties and protections in place to enforce them, and private industry are far more capable of being cyber-responsible than government, as well as more likely to be trusted. Take the TDIF away from DTA – the current (their 4th failed attempt) is a wreck again, and enough-is-enough!

A trusted marketplace with skilled professionals;

1. "as visible and trusted industry standards, do not yet exist in most cases." – not true - AAL3 Authentication for example, the NIST sp800 suite, OWASP, etc.
2. "Trust" is an interesting problem: many vendors lie, deceive, or twist truths, and most providers (and government!) do not do what they say (pretend to be secure or care about security, when the truth is different - they do not care about the customer, they care about themselves - if they care at all.)
3. Some cyber training standards are woefully outdated (I quit my CISSP when many of their lessons I knew to be wrong, and I discovered they had no mechanism to correct them!)
4. There needs to be more adoption of security technologies, and less hiring of professionals to re-invent the wheel – particularly in Government.
5. If better cyber products were used, and improved compliance existed, there would not be such a crushing need for more professionals.
6. More penalties and enforced liability might help improve.
7. Survey our cyber market. Find out who is in it and what we do. Make knowledge of our solutions available throughout government, and BUY our products when appropriate.

A hostile environment for malicious cyber actors;

1. Block threats first – get rid of all the confusing dozens of cyber reporting entities – re-deploy all those now out-of-work staff on prevention duties.
2. There is VASTLY too much focus on detection, deterrence, and response (indeed – page 8 – you did not even list prevention whatsoever!) – get your priorities right – PREVENTION IS BETTER THAN CURE.
3. More law capability is not needed – existing capabilities' are simply not used right now (and are unreachable)
4. We need a working, privacy-respectful, local (and preferably global) digital identity infrastructure. Take TDIF away from DTA and engage Industry to solve this. With strong working Identity, almost all malicious online crime is eliminated.
5. Levy a per-customer mitigation fee on all companies providing inadequately-secure services (e.g. no AAL3) to Australians.
6. Penalties against Australian operators linked to foreign operators who support attacker infrastructure (e.g. amazon hosted penetration scanners, GoDaddy-registered websites hosting unauthorised vulnerability exposures, etc).

A cyber-aware community;

1. COMPLETELY WRONG APPROACH. See above – stop blaming the victim.

Other issues

1. "best practice behaviour change campaigns" (p.17) – Wrong approach – stop blaming the victim.
2. Measurement is not taking place, or is being suppressed/classified:

- The last public report covering government intrusions was in 2013, where Government-server intrusion (63%) dwarfed all other incidents. Since then, Government is being increasingly silent, while passing laws compelling enterprise to be more open.
- Problems can't get fixed while they're hiding under the carpet!
- The 9-month-late "Review of national arrangements for the protection and management of identity information" and associated submissions has not been released. Why not? Why is it more important to avoid government embarrassment than it is to protect Australians ?

Background to my recommendations:

My extensively annotated copy of the Call-for-Views paper contains all my notes: It's the first file here: http://chrisdrake.com/for_gai/

Comments - 2016

1. There is little or no examination of failure – particularly in Government.
2. This is far too much spin doctoring of alleged "achievement", and most rhetoric (especially government) bears little resemblance to reality.
3. Measurement is not taking place, or is being suppressed/classified. When no empirical study of the efficacy of actions is done, nobody can possibly know if their actions are working!

My observation of failures from the 2016 strategy:-

I should not have had to do this – your discussion paper should have included all failures AS WELL as the alleged successes. Not knowing that it failed is itself a fail (failure to measure).

Page 3:-

"this Strategy will help bring more Australian technologies to market" – did it? Can I see the list?

"boosting STEM participation" – did it? Are there numbers? My google search today shows no fix.

"support and create innovative Australian companies." – how was this done? Where is the list of who benefited?

"The Government will show leadership" – where are the statistics measuring government cyber incidents?

ACSC – "will ensure cyber security is given the attention it requires" – is there a report? What incidents did they attend? How many departments comply? Why do they never reply to incident reports unless threatened with FoI? Why are inquiry submission suppressed? Why are cyber reports classified?

"This strategy will develop partnerships between the Australian public and private sectors" – did it? With whom?

"… support home-grown cyber security capabilities" – did it? Which ones?

"We will change and adapt when needed" – have you? In what areas? Who decides "when needed"? What percentage of Government departments fully comply with the ISM and all ASD mitigation strategies? Who is auditing government self-reporting of compliance? Who is being disciplined for misrepresenting compliance?

"I look forward to working with [..] the private sector" – did he? Who? All my approaches were rejected.

Page 2:-

“While governments can take the lead in facilitating innovation and providing security”. What innovation has it facilitated? What security has it provided? N.B. Advice is not security, especially when efficacy is unmeasured.

“The rate of compromise is increasing and the methods used by malicious actors are rapidly evolving”. True and true; unfortunately, security adaptation is not happening: adoption of evolved security is not taking place, and far too much effort is going into cover-ups, victim-blaming and fake security statements instead of revealing the increasing failures.

Page 4:-

“We must embrace disruptive technologies;” which cyber ones has Aus Govt “embraced” since 2016?

“the Australian Cyber Security Centre has lifted Government capabilities to a new level” – this, in my extensive experience, is untrue. Govt cyber capability is almost non-existent in the half-dozen departments I’ve tried to reform over the last 4+ years.

“banks and telecommunications companies, have strong cyber security capabilities” – not true in my vast experience, plus, what “capabilities” they have are targeted at protecting themselves, NOT their customers. This is not my opinion, it is my observation, plus it is stated company policy from multiple banks I’ve spoken with.

Page 5:-

“The Australian Government will take a lead role”. Who lead this? With whom were partnerships forged?

“Australia’s cyberspace must also be a shared responsibility. It will be important that businesses … work with governments … to improve our cyber defences and create solutions to shared problems”. Yes, very important, but HOW do we do this? Cyber-procurement is a total shambles, "build instead of buy" rules all major projects, and there seems to be no genuine consideration of "value for money". Vendors should not have to know who in government needs their products - *Government* should know they need them (e.g. because it's in the ISM or "Essential 8" etc), and they should find us to buy from.

“Strategy’s initiatives will be reviewed and updated annually and the Strategy reviewed and updated every four years.” – was it? Who lead the reviews? Where can I read them? What was measured? Why was I not invited to help? Where are the updates?

“[Actions]will be co-designed with stakeholders from the private sector” – which ones were? Who from the private sector was involved? Why not me?

“Many of these actions also rely on working with all Australians—because we all have a part to play” – WRONG WRONG WRONG. This is the most annoyingly misguided advice that keeps rearing its ugly head time and again. Good Cyber Security is EXTREMELY COMPLICATED, and the vast majority of opportunities to protect everyone lies NOT with the end users, but with their providers. Telling everyone, end-=users and providers alike, that it’s the role of the end-user to be safe, is educating the providers that it’s OK to keep blaming the victims, even when the providers don’t give those victims adequate security in the first place. **Individuals need to be protected**. It is blatantly irrational to hope that 25,000,000+ Australians can all become cyber experts to keep themselves safe. If any of them “have a role to play”, the only reason is because someone did not give them adequate protection in the first place. If you don’t know what that protection is – there is a major failure in your cyber strategy: it should NOT be the Job of a solution vendor to educate the market, least of all the government, and not at all any government purporting to provide cyber-education. That Government should know what’s out there to solve critical problems, especially when it’s Australian-Made, it should be using this itself already, and it should be promoting it, or even mandating it, to every provider who has Australian customers.

“This Strategy charts a new way forward for Australia’s cyber future, one that is creative, collaborative and adaptable.” – there is still too little collaboration, and what exists is far too one-sided (and sometime not even genuine), most severely lack transparency, and are immune to correction when wrong.

Page 6:-

“Cyber Partnership” – ministers are almost entirely unavailable, and do nothing to help in cyber situations. They do not appear to read (or maybe receive) my senate-inquiry submissions. They don’t return my emails or phone calls. Our voice in meetings does not seem to make any difference, and I am not invited to most meeting in the first place.

“We will also sponsor research to better understand the costs of malicious cyber activity” - This needs involvement of a statistician, and to get rid of the time-wasting burden placed on victims. “Doing nothing” when a victim reaches out for help, other than wasting an hour of their time collecting statistics that will never be acted upon is disgraceful.

“We will better **detect, deter and respond** to cyber security threats” – nice, but, this is missing the MOST important part: “PREVENT”. In my vast experience, there is little to no “respond” taking place.

“Australian governments and the private sector will work together to share more information” – this is broken. I’ve been repeatedly blocked, as have others under the excuse “vendors might obtain commercial advantage”. We make the products that keep you safe. Excluding us when you’re under attack is plain crazy.

“streamline the cyber security governance for Commonwealth Government agencies and clearly identify lead responsibilities.” – in my **vast** experience to-date, this is absolutely not happening. Australian government rhetoric surrounding cyber-security practices and the handling of citizen identity information bears almost no relation whatsoever to actual department practices. Rules are almost never followed, security issues are practically never addressed, failures are covered up, inquiries are misled, and there exists no working mechanisms to correct mistakes or fix security problems. Citizens are fed blatantly false assurances regarding the cyber security posture of government departments, usually from anonymous and unskilled sources, who refuse to be identified when challenged. There are no penalties for ignoring the rules, Departments routinely refuse to correct cyber issues, and cyber testing is rare and usually fails. In the comfort of anonymous or private forums, many government cyber professionals express these same opinions, along with their frustration and not being able to compel departments to change.

- Every department I’ve contacted (AEC, DHS, ABS, ASD, former DTA, PM&C, AUSTRAC, Defence, ACSC, plus some state and local governments, and others I’ve forgotten), no exceptions, point-blank refuses to fix any of the large number of cyber security and privacy issues I’ve brought to their attention.
- Almost every department claims that they have no security problems (despite **evidence** to the contrary that I supply).
- All department claims of "we have no security problem" are unsigned, unattributed, and obviously not from any security professionals.
- All departments routinely block every FoI request I make (all relate to cyber-security failures).
- Departments censor (remove) all controversial public comments that are made on systems they control, especially ones relating to cyber security.
- No departments I’ve found appear to have any actual ITSA or similar (supposedly mandatory) roles with staff actually in them (I did notice an advert appeared seeking to fill one of those roles after I began applying pressure - so perhaps I made one tiny bit of difference to one department there).
- Departments all refuse to identify any of their IT security staff - they refuse to name names, they refuse to provide contact details. My conclusion: they do not have staff in these roles.
- The OAIC FoI review process is a sham (backlog of 1+ years, and no power to right wrongly refused FoI reports anyhow).
- There appears to be a highly organised FoI "officer" scheme or training in place to block every request that might embarrass government from being honoured (despite the law clearly banning that behaviour).

- "Consumer Protection" laws do not apply to government: when government break them, all action I've taken to right those wrongs has resulted in department lawyers telling me the sections of legislation that make them exempt.
- All senate inquiry reports that embarrass government become deemed "confidential": this is a way to hide the content AND EXISTENCE of these reports from everyone - they are removed from the record, they are never available to anyone. From observation of inquiry broadcasts over the internet, senators appear not to be provided with these reports (or at the very least -they do not read them).
- Every inquiry senator I contacted failed to confirm they ever read or received my submissions.
- I never get invited to participate in anything I apply for (to give evidence at inquiries, or to participate in reporting).
- As best I can tell - all inquiry and report-writing that takes place is not genuine. This includes the PM advisory panels I did manage to be on. They have an agenda "get some law or other passed", and industry involvement in the process is a sham - simply so government can pretend they consulted before they did what they already have planned.
- Some departments providing security advice to citizens source dubious content from the internet to base their advice on, and then refuse to be corrected when they're wrong, refuse to acknowledge evidence proving them wrong, refuse to study the efficacy or suitability of their advice, censor criticism about their flawed advice, refuse to publish corrected advice, and continue repeating their advice despite the volume of material weighing against them.
- Most departments actively mislead the public about their security and privacy practices – for example – the DTA web site in relation to the TDIF, under the heading "How we protect your privacy", linked to a privacy impact assessment (PIA) document – giving the false impression that this document proved that the DTA protected privacy, when in reality, inside the PIA details it actually reported that the DTA **failed every single privacy control that was tested**.
- Australia Post, a government-owned "body corporate" existing through specific government acts, is considered a "commercial entity", and thus it is allowed to escape FoI scrutiny.
- The Australian Signals Directorate (ASD) – our peak body informing all other departments on the topic of cyber security, is immune to FoI scrutiny too.
- Public servants are highly misleading when appearing in senate inquiries: they fail to report their own mistakes, and they readily point to industry failures as a means to divert attention from their own mistakes, and some departments cover up the failures of other departments when questioned by senators (e.g. The ASD head, when asked in the government-service-failure inquiry if a department was compliant with ASD advice, chose a lengthy reply summarising ASD advice as his tactic to avoid answering the question, which worked).
- The way the privacy law is written gives all departments a "get out of jail free" excuse not to fix security problems: the ASD (who provide security advice, including the operation/oversight of so-called "approved" secure cloud etc) is not the same department as the ones *with* the privacy data, so no single department has security responsibility over this data, so no department is ever in breach when it's insecure.

A. Australian Government systems are utterly insecure (this is a well-reported fact - 62% of Australian cyber break-ins are to Government servers. That's 4 new ones every day. Sources: Australian Signals Directorate "Cyber Picture 2013" and DPM&C Strategy page 16:
B. There is no working mechanism to fix it.
C. There is no motivation to fix either of the above.
D. Senate inquiries pertaining to government failures are 100% whitewash - public servants totally control these, and they do not rat on their own.
E. Reviews and inquiries never seem genuine, and always exclude me and the submissions I make - uncovering public service failure appears never to be acceptable in final reports.
F. Nobody in the public service seems accountable - there are no penalties for doing the wrong thing.
G. The system in place to cover all that up is well oiled.

I have hundreds of documents verifying all my above claims which contain even greater numbers of embarrassing problems that the few above that I've recalled.

- Here's how ASD lawyers responded to me when I submitted a privacy complaint regarding their approved systems being implemented with no security whatsoever to collect voter enrolment details.

> " As the ASD does not have possession or control of a record containing your personal information collected by the AEC, my initial view is that the ASD is not required to take reasonable steps to protect the security of such information. "

That bears repeating in bold. It is the *written* advice FROM the ASD - Australia's body responsible for cyber security in government, that: " **THE ASD IS NOT REQUIRED TO TAKE REASONABLE STEPS TO PROTECT THE SECURITY OF** [VOTER] **INFORMATION** "

Page 7:-

“co-design national voluntary cyber security guidelines” – these are outdated, with wrong information. They probably need to include recommendations to products and vendors to actually work.

“shut down safe havens for cyber criminals.” - How many attacks reported by Australian personal (non govt, non business) Victims got shut down through these mechanisms? Is there a list of the attacks reported (e.g. phone scams, ebay fraud, ransomware, etc). Every attempt I’ve made to shut down scams and frauds has met with no success, and I’ve tried *hard*. I’ve worked with the FBI on USA fraud, and they got results. Why can’t we?

Page 8:

“the Government will also support Australia’s cyber security sector to expand and promote their capabilities to the global market.” - Did it? Can the Government supply a list of who is in this sector, and what they do? Trick question: I know they cannot. I've never been surveyed for example... Who, if anyone, in my industry benefitted from this? Where was the promotion done? Why has nobody in my government ever contacted me for either my advice, or to use my products? How many other Australian Vendors have also never heard from anyone in our government who needs their solutions? With no exception, every successful Australian Cyber business I’ve asked (a lot) has said they owe their success to leaving Australia and selling overseas.

“With better focussed cyber security research and development” – we do not need more research – we need commercialisation; almost everything you need already exists in Australia – what is needed, is for Government to USE IT.

“Cyber Security Growth Centre” – major failure. They have never even surveyed our industry – they’re supposed to grow us, but have no idea who we are or what we do, no regard for the size of our country or where vendors are located or the costs to vendors trying to use their services.

“particular focus on support for cyber security start-ups” – which ones? What support did they receive? How many government departments are now buying products from those start-ups? If none, why not?

Page 9:-

“The Government will also further improve national cyber security awareness and work to ensure all Australians understand the risks” – WRONG WRONG WRONG – see my explanation earlier.

I invite you to peruse some of the public submissions I have made to assorted government inquiries and reviews. Every one of these has been “suppressed”, along with the records of me making these submissions.

Find them here: http://chrisdrake.com/for_gai/