THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
CREATE CHANGE

The University of Queensland's submission to Strengthening Australia's Cyber Security Regulations and Incentives

Introduction

The University of Queensland (UQ) is in the world's top 50 universities and is renowned for the quality of its teaching and research, it also hosts the national not-for-profit security group, the Australian Cyber Emergency Response Team (AusCERT). AusCERT is Australia's pioneer cyber emergency response team and it helps members prevent, detect, respond to, and mitigate cyber security incidents. UQ is home to UQ Cyber Security, a multi-dimensional group of 50+ academics and researchers from various disciplines, from secure quantum communications to researching policies addressing the global cyber security skills shortage, that conducts interdisciplinary research and partners with international organisations to address the biggest challenges facing cyber security around the world. UQ appreciates the opportunity to contribute to the submission paper Strengthening Australia's cyber security regulations and incentives', an initiative of Australia's Cyber Security Strategy 2020 and the collaborative nature of the Government's engagement in this important area.

Area 1: Setting clear cyber security expectations (*mandatory or voluntary cyber security standards for corporate governance, smart devices (internet of things) and personal information*

Governance Standards for Large Businesses

Although there is always the question of whether a voluntary approach, as opposed to a compliance approach ever works, it is a good place to start with, at least. We would be looking to see some sort of voluntary governance standards initially. It should be voluntary but the reality is, this will likely become enforced indirectly by cyber insurers and one of the questions people will ask is whether the standards are followed and how are we conforming to the government standards. Therefore, cyber-insurers will reach for that.

There is a concern that this may be too open-ended for large businesses. Relating to this, the definition of 'large business' may need to be clearly defined. For instance, is it the $3m turnover requirement for the Privacy Act (Cth)? We believe the definition of these principles and clear guidelines will be key. In short, we think we should start with voluntary and if that incentive is not enough, perhaps move into mandated standards. If a voluntary governance standard can be established, this will go towards proving reasonable action later – should there be an actual dispute around damages. If large businesses can prove that they were trying to conform with these voluntary standards, it can be assumed that they had reasonable measures in place, as it is common that regulations have some form of reasonable practices in place. Also, co-designing with industry might not be enough but engaging action bodies and other stakeholders within the industry to help co-design some standards might be a good idea. In any case there needs to be some sort of definition of what a correct standard is.

Minimum Standards for Personal Information

We agree that we need a specification of minimum best practice approaches. These need to be clear, though probably not legislated as best practice changes all the time. The Privacy Act itself needs to be enhanced as it is pretty outdated and this was established and conceptualised under a different sociotechnical environment, and only applied to a certain range of government entities and large businesses with a $3mil turnover. Hence, there is also a question of whether that should be expanded irrespective of a turnover.

Currently, the Privacy Act can only be mobilised to make a complaint by an individual and requires the release or registering of data breaches, so this is not really a cause of action for an individual whose private information has been released. There are potentially other areas of law like torts that can apply to this situation but the act itself does not provide any protection of individuals with any other measures other than file a complaint. The Australian Information Commissioner is also limited in the types of fines they can levy against companies that are not meeting their obligations. Currently an organisation does not get fined for a data breach, they only get fined for

not reporting a data breach. This is an issue of transparency. One concern with the current data breach notification regime relates to the requirement that 'serious harm' is conceived of as the harm that is experienced by a single individual and not in terms of collective harm. This leads to problems, in that the legislation does not provide a cause of action when a large group of individuals experience small individual harms resulting in a substantial collective harm. For example, a data breach causing $100,000 in harm to 100,000 people is likely not serious harm and so not reportable. In contrast a $1000 breach that affects only two people is likely would be reportable. This leads to enforceability problems for the Office of the Australian Information Commissioner (OAIC). The code is only effective as it is enforced, and other jurisdictions outside Australia have much stronger codes. We agree this needs to be enforceable. Perhaps an integrated legislation that is clear about all different sectors and obligations instead of having it in different areas, and making it very clear on what is required will make people more likely to follow it and this to be enforced. On a side note, the Australian Communications and Media Authority (ACMA) is quite happy with a code on Internet Service Providers.

With regard to technical controls and technologies, we would advocate for the Essential 8 from the Australian Cyber Security Centre as a minimum baseline. However, the biggest issue is the social engineering problem, hence we need some type of technical controls addressing these social engineering risks. We also need some type of technical control to ensure companies are responsible for managing personal data they collect that is identifiable, that aligns with the measures taken under the Privacy Act.

Another suggestion is that we need to be able to provide users or owners of the personal information the option to opt for transparency or the usage of their personal information not just locally but also globally if they operate overseas e.g. global tech companies. Ensuring that companies that collect the data have responsibility and awareness of the responsibility for the data collected is also necessary.

Mandatory Product Standard for Smart Devices

We agree the possible approaches you listed in the submission paper (no universal default passwords, vulnerability disclosure policy, secure software updates) is good.

One missing part is around the expectation of privacy for the people using it. For example, do the suppliers disclose this or do we set expectations or is there a way we can report them?

Another missing part is the privacy of the users' information, as there is no current expectation from legislators for smart devices to inform users about potential privacy risks. The manufacturers and suppliers that collect a lot of private data via smart devices have no features promoting or improving privacy awareness (e.g. if you hook smart devices at home what are the potential information you are sharing?).

The consideration of security issues of communication between smart devices is also not mentioned here. Another issue is cryptography (algorithm, key length, etc.) as smart devices have limited storage and resources so they tend to use weak cryptographic schemes, and there must be better security guidelines. The idea of having a star rating (e.g. like the energy star ratings) that is linked to other recognised standards that corresponds to global standards will be useful. For certain industries like manufacturing of small devices, it can be legislated so these producers have a higher responsibility as consumers have less access to this information, but the establishment of this can be costly.

There is a concern about the definition and scope of smart devices as well. We need to be sure that we understand what is and what is not a smart device - are IoT type devices caught. We agree with mandatory standards and believe that the next step is transparency. A simple example could be to have stickers to post on smart devices that prove a certain level of rating. Lastly, how do we enforce privacy and security expectations on the overseas provider of goods and services?

Area 2: Increasing Transparency (through cyber security labelling for smart devices, health checks for small businesses, and improved disclosure of software vulnerabilities)

Labelling for smart devices

Yes - there should be mandatory labelling, physical and digital stickers.

Responsible disclosure policies

We strongly recommend a voluntary guidance. There needs to be some guidance on the government responsible disclosures, and people who are finding these vulnerabilities need some form of protection.

The government needs to have a nation-wide responsible disclosure policy; otherwise cyber security professionals will not know how to report potential security issues and how companies can act towards this. The policy will benefit the business and industries, and secondly regulate the behaviour of cyber security professionals.

There is a question around the feasibility of the framework for all organisations, since organisations adopting responsible disclosure programmes should have the resources to do this. On the other hand, will this cripple the businesses of SMEs? Perhaps a voluntary guidance will help but it will depend on the classification of businesses.

One missing gap in terms of government responsible disclosure, is that there needs to be clearer guidance around reporting processes (when and how to), and the assurance that the reporting person isn't labelled badly as someone who is trying to hack the government system. There was a similar case in New Zealand where an ethical hacker was apprehended as he found certain vulnerabilities in their government IT systems and was jailed by the Minister at the time. There is also a bit of fear for the people who report and try to do the right thing. For this we suggest maybe empowering the regional, industry or national CSIRTs/CERTs that have the ability and scale to take on this role to relay these messages (e.g. AusCERT). We also strongly support the adoption of responsible disclosure policies among Australian businesses.

Voluntary health check for small businesses

We think this means cyber health, but 'health' needs to be defined so that it can be measured and assessed. Also defining 'small businesses' is critical.

As incentives for small businesses, we suggest having a pathway for small businesses towards maturity. For example, stage 1 can be meeting the Essential 8, then stage 2 and 3, and stage 4 obtaining the ISO certification. This is the approach by the Singapore government.

For some small businesses that don't have capacity or resources, perhaps the government will need to do more to help through financial incentives such as no costs to do this or giving tax breaks for entities who do this. It really depends on what is defined as small businesses and the type of business they do. For small businesses, the commercial benefits may need to be proved via some means (e.g. cyber aware badge/sticker), so the person doing the checking has some form of legal coverage if it turns out that the business weren't so cyber good after all (liability issue).

There are several other issues – we need to ensure this method is authentic as do not want a false sense of security, concerns that a legal liability may exist for the person that is doing the health check, a question of trust if no fee involved. Perhaps a 250/500 or some type of subsidy scheme where we still have small businesses pay something so that it is worth something (the 'green beret' idea) might be good. Not to mention the possibility of bad actors interfacing small businesses (e.g. if you already have limited resources to cyber security you are

opening the possibilities for bad actors to extract personal information) so stronger implementation is needed. I If something is voluntary to a business, they are less likely to act hence leaving the business vulnerable to phishing attacks and security breaches due to lack of skills. If it is mandated, the chances of businesses taking preventative measures will be higher, rather than waiting for someone to provide guidance.

Area 3: Protecting Consumer Rights (through clear appropriate legal remedies for victims)

Clear legal remedies for consumers

Clear legal remedies are a much better idea, as if it is just generalisable without clarity then you are waiting for a risk-taker plaintiff or one case to define what that is and not every dispute gets to that point. There will just be a lot of lack of clarity until a perfect case comes up. Having that clarity around what constitutes a breach will help minimise that risk and can provide greater guidance to people in need.

One issue in this space is that a consumer will not choose to go through a lengthy trial, and probably class action lawsuit will be the most viable option but generally people will agree on a small amount (e.g. $1000) to settle and avoid legal action.

Australia is not much of a litigious society but having a legislation and definition to help clear the boundaries is better than nothing. There is no clarification around the right of action for privacy breaches or any implications there will be a damage. Some type of small claims tribunal for cyber security may be an option.

Contributors from UQ

Prof Ryan Ko, Chair and Director of Cyber Security, Deputy Head of School (External Engagement), School of Information Technology & Electrical Engineering

Dr Micheal Axelsen, Senior Lecturer, Business Information Systems, School of Business

Dr Allison Fish, Senior Research Fellow, Centre for Policy Futures

Adjunct Professor Nick Tate, Cyber Security, School of Information Technology & Electrical Engineering

Mr. Geoffroy Thonon, Principal Information Security Analyst, AusCERT

Prof Claudio Mezzetti, School of Economics

Dr Guangdong Bai, Senior Lecturer Software Engineering, Cyber Security, School of Information Technology & Electrical Engineering

Dr Naipeng Dong, Lecturer, Cyber Security, School of Information Technology & Electrical Engineering

Dr Thomas Christy, Lecturer, School of Information Technology & Electrical Engineering

A/Prof Frank Zhang, Accounting, School of Business

Ms Kana Smith, Project Manager, Cyber Security, School of Information Technology & Electrical Engineering

Contact details

Prof Ryan Ko
Chair and Director, Cyber Security

M +61 **455 110 302**
E **ryan.ko@uq.edu.au**
W cyber.uq.edu.au

Ms Kana Smith
Project Manager, Cyber Security

M +61 **439 718 135**
E **kana.smith@uq.edu.au**
W cyber.uq.edu.au

CRICOS Provider Number 00025B