Australia's 2020 Cyber Security Strategy
Response

Submission date: November 2019
Submitted by: Preston de Guise

"Enterprise Systems Backup and Recovery: A Corporate Insurance Policy"
CRC/Routledge Press, 2008, 978-1420076394

"Data Protection: Ensuring Data Availability"
CRC/Routledge Press, 2017, 978-1482244151

"Protecting Information Assets and IT Infrastructure in the Cloud" (co-author)
Auerbach Publications, 2019, 978-1138393325

"Data Protection Blog"
Self-published, Blog, 2009-2019+, https://nsrd.info/blog

Introductory Comments

I welcome the Australian government seeking feedback from the public as it prepares its 2020 Cyber Security Strategy. In this response, I've drawn on my experience as an industry expert in data storage protection. I have worked with Australian businesses of practically all sizes to design and assist in the deployment of data protection and recovery services. As such, I hope the insights I've gained from businesses regarding security, privacy and data loss are useful.

"What customer protections should apply to the security of cyber goods and services?" and *"What needs to be done so that cyber security is 'built in' to digital goods and services?"*

In terms of customer protections for cyber security, I'd recommend the following minimum protections. (Some of these are at odds to current government policy.)

Encryption

There should be a reasonable expectation that devices and communications use encryption.

- Devices that store data (e.g., smartphones, tablets, computers) should ideally include an option to encrypt that data.
- Devices that transmit data should preference, or ideally only transmit using end-to-end encryption.
- Encryption keys should be stored in such a way that they are inaccessible to the vendor(s) providing the devices or services.
- The government should roll-back, and fix its encryption legislation (2018 "Assistance and Access Bill"). While government officials almost singularly argued in the media that this legislation was to target illegal activities such as terrorism and child abuse, it has far-reaching effects that the government refused to discuss or acknowledge. The legislation was ill-thought, contrary to industry expert opinion, and has already caused damage to Australia's reputation. It also directly *reduces* the Cyber Security profile of Australian citizens.
- There should be a legislated requirement for encryption at rest and in-flight of all data held on Australian citizens – by government agencies or private businesses unless permitted otherwise by an exclusion policy:
    - Such encryption must include both primary copies of data, and any backup copies of data.
    - It should be planned as a phased introduction over 3-7 years to accommodate standard capital refresh cycles in businesses.
    - The government could encourage faster adoption by offering incentives to businesses that achieve the transition in under 3 years.
    - The process must cover *all* Australian businesses, including small businesses that might otherwise be exempted based on employee count or annual revenue. The government could assist smaller businesses in this process by establishing an information website. The website would be specifically aimed at businesses with no IT staff, and provide simplified details, such as explaining encryption and where to use it, and how to enable it in standard desktop operating systems.

Privacy

Privacy breaches are often an entry point for a targeted breach of an individual's security. As such, promoting and ensuring a high standard of privacy will naturally lead to enhanced security, for individuals and businesses.

- The mandatory breach reporting laws (which became active February 2018) allow businesses to take up to 30 days to advise individuals if they have had a breach. This period is too lengthy and should be a maximum of one week.
- Australia should look towards the European General Data Protection Regulation (GDPR) as an example of enshrining a right to privacy in legislation, which will have a positive impact on overall Cyber Security within the country. At minimum, all Australian citizens should:
    - Be able to find out what data a business holds about either them[1]. This would include a "metadata" overview ("we hold your date of birth, name, address, and tax file number"), and an optional data extract (to be provided securely)
    - Ask to be permanently removed from data holding, where compatible with other legislation. (I.e., someone with a home loan can't ask to have their records deleted. However, someone who has shopped once at a store and started to receive marketing material should be able to ask for their contact details to be permanently erased.)
- Electronic mailing list laws should be strengthened to require someone to explicitly sign-up rather than sign-up being implicit to a particular action. For instance, the retailer **Kogan** (kogan.com.au) automatically signs up customers to its mailing lists as a result of making a purchase. Such automatic sign-ups should be prohibited – consent must **always** be explicit. In particular:
    - If a company desires a customer to sign-up to their mailing list during a purchase process, they should explicitly include a check-box or other option for a customer to agree to that process, *and*
    - Completing the purchase should not be contingent on signing up to electronic mailing lists.
- On-line sales vendors should be prohibited by law from saving credit card information for customers who are making a transaction unless the customer explicitly consents to this.
- Any business that holds credit card details should be required to notify customers (at least half-yearly) customers that their credit card details are stored.

[1] There would have to be considerable protections made if legislatively people could request the same data of others for whom they are the legal guardian. For instance, while parents might reasonably expect they should be able to make this inquiry on behalf of a child, this should include protections in instances of personally sensitive information. A teenager for instance who believes they might be LGBTI should be able to talk to a medical professional without concern that their parents could demand records of those discussions.

The notification should include a phone number or URL that can be accessed to request the deletion of the credit card information. (Obviously, this should not include details of the credit card itself.)

Promoting more secure devices and services

Within IT and IT security, the term "hardening" applies to situations where additional configuration steps can be performed to a system or device post-installation to present a stronger security posture. This hardening process can include activities such as turning off non-essential services running on the system, restricting permitted network ports, and setting more stringent controls over user accounts and passwords.

Arguably, younger generations with a 'lifetime' exposure to technology (e.g., Gen Z, Millennials) may have at least a peripheral awareness of computer and network security[2]. However, it is also the case that network and device security can be a challenging topic, able to tripping up even IT experts. Consumer protections should, wherever possible, be built into cyber goods and services, rather than expecting consumers to "harden" a service or device to render a *modestly* secure system.

There is increasing sophistication in the security of standard operating systems and smartphones/tablets. Companies behind consumer operating systems (Microsoft, Apple and Google) have by and large increased their security profiles – though we should be mindful that enhanced security requires a robust approach to consumer data privacy as well.

However, while these companies may have moderate to sufficient approaches to security, there always has been a perhaps lackadaisical approach to device security from a variety of other vendors, such as:

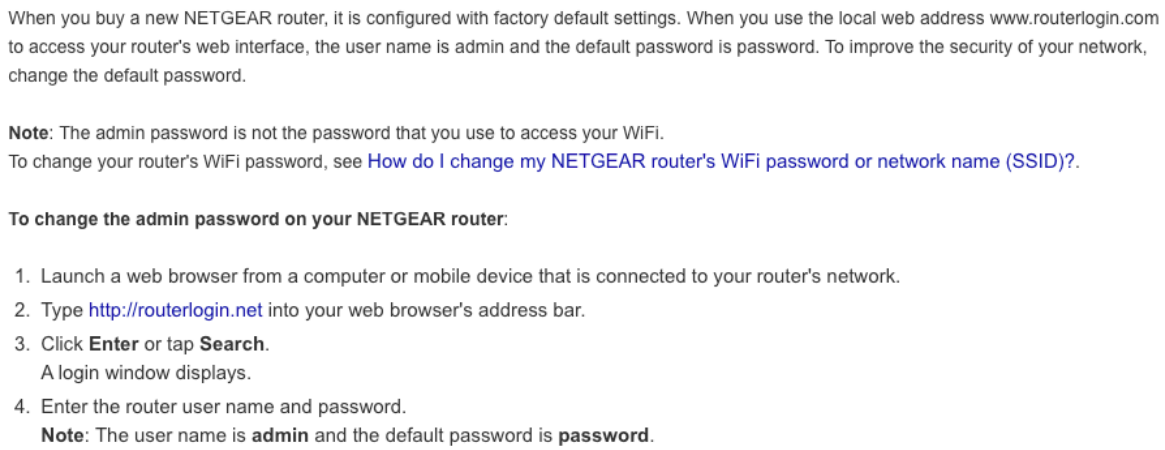
- WiFi security cameras
- IoT ("Internet of Things") device suppliers
- "Smart" household items (e.g., refrigerators with built-in Internet services)
- Printers
- WiFi routers
- ADSL/NBN modems and routers

All too often, these types of devices come with standard passwords, and there is little or no incentive in consumers to change those passwords. More so, there's rarely any *prompting* by the vendor, either. Without this prompting, it's likely that few regular consumers using these services or devices would even consider the need to change these passwords.

[2] Compared to generations that have had less experience or generally experience less confidence in computers, as a result of only experiencing them in adult life – baby boomers and older Gen X in particular.

These types of devices, if improperly secured, can allow data exfiltration, virus/malicious software installation, or other forms of private network penetration. Sadly, for many, "improperly secured" can be synonymous with "standard configuration".

Many of these types of devices have a static default administrative password that is well documented or easy to find. A Google search for "default admin password for Netgear router", for instance, leads to the article shown in Figure 1 (page 6).



When you buy a new NETGEAR router, it is configured with factory default settings. When you use the local web address www.routerlogin.com to access your router's web interface, the user name is admin and the default password is password. To improve the security of your network, change the default password.

Note: The admin password is not the password that you use to access your WiFi.
To change your router's WiFi password, see How do I change my NETGEAR router's WiFi password or network name (SSID)?.

To change the admin password on your NETGEAR router:

1. Launch a web browser from a computer or mobile device that is connected to your router's network.
2. Type http://routerlogin.net into your web browser's address bar.
3. Click **Enter** or tap **Search**.
   A login window displays.
4. Enter the router user name and password.
   Note: The user name is **admin** and the default password is **password**.

Figure 1: Netgear Knowledgebase Article, "How do I change the admin password on my NETGEAR router?"
https://kb.netgear.com/20026/How-do-I-change-the-admin-password-on-my-NETGEAR-router

A simple Internet search for "default admin password for X", where X is a vendor and product, such as shown previously, shows that this is not 'secure' information in any way.

More mature consumer goods businesses provide processes that allow better default security for devices. Newer Internet-accessible Web cameras, for instance (often used for simple self-service home security and monitoring) often enforce a setup model premised on having physical access to the device. In such situations, it might be that:

- Initial setup by scanning a QR code on the device, using a smartphone app, or
- The default admin password is the device serial number rather than a hard-coded word such as 'admin', 'password' or 'changeme', and
- Users are more likely under these circumstances to be prompted to set a password for the devices that must be known to access them.

While this is not to say the security of these devices is beyond reproach, it creates a higher degree of security than enabling the devices to be scanned using a standard list of passwords.

Requiring all vendors of consumer goods selling into Australia to change their embedded system security designs, though desirable, is of course highly unlikely to be practical in its effects given the sheer number of vendors, and the potential for ordering overseas for Australian delivery.

Two examples of options that might be used to achieve change on this front are outlined below:

1. Security Quick Start
    a. Vendors of consumer goods vendors sold into the Australian market should be encouraged to always include with their products a "Security Quick Start" information sheet.
    b. This guide should at most be a single A4 page, that describes in lay-terms what steps consumers should take when setting up their device to secure it.
    c. In the most basic scenario, this might be details of how to change any default passwords, include recommendations for password security, and provide the support contact details for customers who have questions.
    d. Product packaging clearly shows if there is a "Security Quick Start" guide inside, and consumers are encouraged via advertising and other promotions to look for that.
2. Security Star Ratings
    a. A more robust approach would be to develop a security rating system, in a similar approach to the "Energy Star Ratings" system that Australian consumers already find familiar.
    b. The security rating might give a ranking from 1 to 5 stars, outlining how the product ranks from a security perspective. For example:
        i. A product might receive zero stars if it has hardcoded passwords that cannot be changed.
        ii. If there are hardcoded passwords that are static across all devices (e.g., the password for the "admin" user is always "password"), then it might rate 0.5 stars, unless
        iii. It includes an information sheet such as the above, in which case it might rate 1 star.
        iv. 2 stars would be if there were default passwords that were at least moderately random or non-simplistic.
        v. 3 stars would require hard default passwords tied to individual device properties (e.g., the device serial number)
        vi. 4 stars would have no default passwords, or default passwords based on serial number, but require a password with standard password rules to be set during installation before the device can be used, and
        vii. 5 stars might be awarded if the device achieves a 4-star rating, can certify all traffic where passwords are specified is encrypted, and also supports additional security options, such as two factor authentication and/or periodic prompts to change passwords.
    c. The number of such devices on the market makes an independent assessment of each vendors products mostly impractical.

d. Instead, it is more likely that vendors would need to 'self-certify' if they enrol into the process, providing a binding statement that they believe they qualify for a particular security star rating based on documented evidence.
e. A government website would outline precisely what criteria a device has to meet to achieve a particular security star rating.
f. That website would also provide a feedback mechanism to allow an individual to provide information if they feel that the rating assigned to a device is inaccurate.
g. It is unlikely this feedback mechanism would be used in the first instance by regular consumers – more so consumers who have a stronger IT background, including actual security professionals.
h. Stores (electronic and bricks & mortar) could be encouraged to provide displays referring to the "Security Star" programme to increase customer knowledge. (This would likewise encourage them to seek products and services that have an appealing rating.)

The second option requires more work and would require the formation or extension of an appropriate body to lead the certification process. It may be as well that certification is not made mandatory. Instead, there is a consumer education programme to encourage consumers to look for the security rating when they are buying devices that are network accessible.

How can high-volume, low-sophistication malicious activity targeting Australia be reduced?

There are many approaches, but I have chosen to focus on one particularly vexing scenario. Let's consider it from the perspective of Alan, who is at work and receives a call as follows:

> *Caller: "Hi, it's Karen from Telstra. How are you today?"*
> *Alan: "I'm good. How are you?"*
> *(Alan has a Telstra account.)*
> *Karen: "I'm well thanks. We've been working on some new account options and we think we've got a better price plan for you, are you interested?"*
> *Alan: "I guess so…"*
> *Karen: "Great! Now, before I get started, I do have to verify your date of birth and account number, please…"*

This call would typically be associated with *phishing* activities, whereby a malicious actor impersonates someone whom a person might reasonably expect (or at least not be suspicious about receiving) communications from.

In this case though, the call is a legitimate one, and it is a depressingly common scenario. It is not the intent of this response to call out Telstra specifically – they may have even abandoned the practice, but it is businesses of Telstra's size and influence that need to be particularly mindful of their social responsibility on this front.

There are a multitude of businesses in Australia, usually in the telecommunications and financial services sectors, who conduct these sorts of cold-calling processes with customers. This is somewhat hypocritical given the nature of these calls train customers to expect such behaviour may be reasonable, given these same companies also conduct security awareness training for their staff over the same types of calls or contacts!

This is certainly one area where the government should legislate. No business should be permitted to conduct cold-calls of customers where they request sensitive or personally sensitive information.

Rather than making these types of calls, businesses who need to conduct these transactions with customers should:

1. Outline to the customer exactly what they wish to discuss.
2. Provide a verifiable means that the customer can use to connect back to the business. For example:
    a. Provide a phone number the customer can call back on.

    b. The phone number should be readily identifiable on the website for the business
    c. If the number goes to a general menu system, they should also provide the sequence of menu options used to get to that particular team, and a case ID to quote
    d. Offer to SMS those details (but no clickable links) to the customer.
3. If the customer does not wish to call back, they should revert to sending an email or letter.

While businesses would undoubtedly find these measures an inconvenience, steps must be taken to encourage people *not* to divulge sensitive information when they are not expecting a call, or a call comes in from an unrecognised number.

Accompanying legislation that prohibits these calls, the government should also run an information programme through advertisements and other appropriate means. This programme would explain to consumers that they should not give out sensitive information unless they have initiated contact with businesses.

Encouraging people to take this security approach will have flow-on effects. Legislation would primarily focus on preventing businesses from conducting these cold-calls, which is a good step towards increased security. The accompanying education campaign would likely have flow-on benefits, creating a situational awareness that also applies to electronic contacts used for phishing attacks.

How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?

An essential approach to modern security is to work on the presumption that perimeter security mechanisms will not always be successful. That is:

- A malicious actor can gain access to an internal network, despite the presence of firewalls.
- Malicious actors may spend considerable time monitoring a network once they have gained access to it before they take any hostile action.
- Virus and malware scanning systems are not infallible

This means that businesses should plan for the inevitability of a cyber-attack, rather than only on avoiding a cyber-attack. I.e., proactive planning on how to best conduct data recovery in the event of a destructive cyber-attack is a precaution that every business, no matter how small or large, should undertake.

It is essential then that businesses are first encouraged, then required, to have adequate data protection plans that include recoverability. The use of cyber-insurance to "pay cyber-ransoms" for instance should be discouraged since it merely ‚promotes a belief among cyber-attackers that there is a market for payment.

Appropriate data recovery services should be used to allow businesses to roll back and retrieve content without having to pay ransoms to decrypt data, for instance. These include:

- Use of snapshots and/or continuous data protection (CDP) techniques for fast, on-platform recovery where an event has happened recently, and
- Use of backup/recovery systems with appropriate security hardening processes to provide an off-platform recovery mechanism.

These requirements would apply to both on-premises and public-Cloud data environments since both are susceptible to cyber risks. Arguably, businesses should have these forms of data protection already. However, the number of ransomware attacks in Australia alone shows that businesses are often underprepared, with issues including:

- Insufficient replication of protection copies
- Protection systems (online and offline) out of support/maintenance increasing risk
- Insufficient security hardening for protection systems
- Insufficient protection storage for all operational data/workloads

While it may be impractical to force rapid change in these areas, the government could look at phased approaches which allow business budgets to adapt, and for

sufficient workarounds to be adopted – not all data has to be protected equally, of course. (Part of the process of managing the cost of data protection is to perform appropriate data classification.)

Businesses should be encouraged to incorporate these data recovery processes into their cyber security strategies. If planned/implemented correctly, they allow a business to recover *considerably faster* than decrypting the data – which allows businesses to get operational again sooner.

What private networks should be considered critical systems that need stronger cyber defences?

The following private networks should be considered critical systems requiring strong cyber defences:

- Power suppliers:
    - Maximum security required within network segments (usually isolated already) responsible for power generation or core distribution
    - Heightened security for "corporate" networks as they represent an obvious point to probe for potential access to the above networks
- Essential emergency services, including but not necessarily limited to:
    - Hospitals
    - Police, ambulance and fire services
    - Outpatient services
- Service/control networks for telecommunications providers, including:
    - Traditional providers (i.e., Telstra, Optus, Vodafone.)
    - Internet service providers
    - NBNco
- Transport hubs and services, including:
    - Road authorities
    - Airports
    - Ports of entry/shipping ports
    - Aircraft carriers
- Dispatch, ordering and warehouse control systems for:
    - Supermarkets (Australia's relative lack of competition in this market means a significant disruption to one of the supermarkets could have a rapid, and substantial impact)
    - Primary logistics operators (not just Australia Post, but courier companies with national reach operating in the country).

Obviously, there are also a variety of local, state and federal government networks that would already be considered essential.

Due to their potential for impact on the economy, Australian Fortune 500 and ASX 100 listed companies should also be encouraged to consider their networks to require heightened sensitivity compared to standard corporate networks.

Education

In addition to the general security concerns regarding Cyber Security incidents, the government has also indicated that part of its approach for a new Cyber Security strategy is the impact that events can have on the Australian economy, both micro- and macro.

While the government is undoubtedly considering short-term and tactical strategies for Cyber Security, it should also evaluate strategic approaches. One such longer-term goal would be to work with the State and Territory governments on ensuring that "Cyber Security Awareness" programmes are built into primary and secondary school strategies.

The goal of these programmes should be relatively straighforward – rather than trying to create a generation of "cyber experts", the approach would be to create situational awareness of cyber risks. Some of this could leverage existing programmes that target cyber-bullying and help children understand that people online may not be who they say they are. Scenarios to explore could include:

- Phishing
- Identity theft
- What constitutes sensitive/personally sensitive information, and why
- Understanding the importance of adequate passwords and security enhancements such as two-factor authentication

Some of these concepts may already exist in secondary schooling computing subjects – however, there would be merits in bringing them forward into the latter half of primary schooling to help grow habits earlier. Effectively this is a 'cyber' equivalent of teaching children to look twice before crossing roads and not to accept rides from strangers.