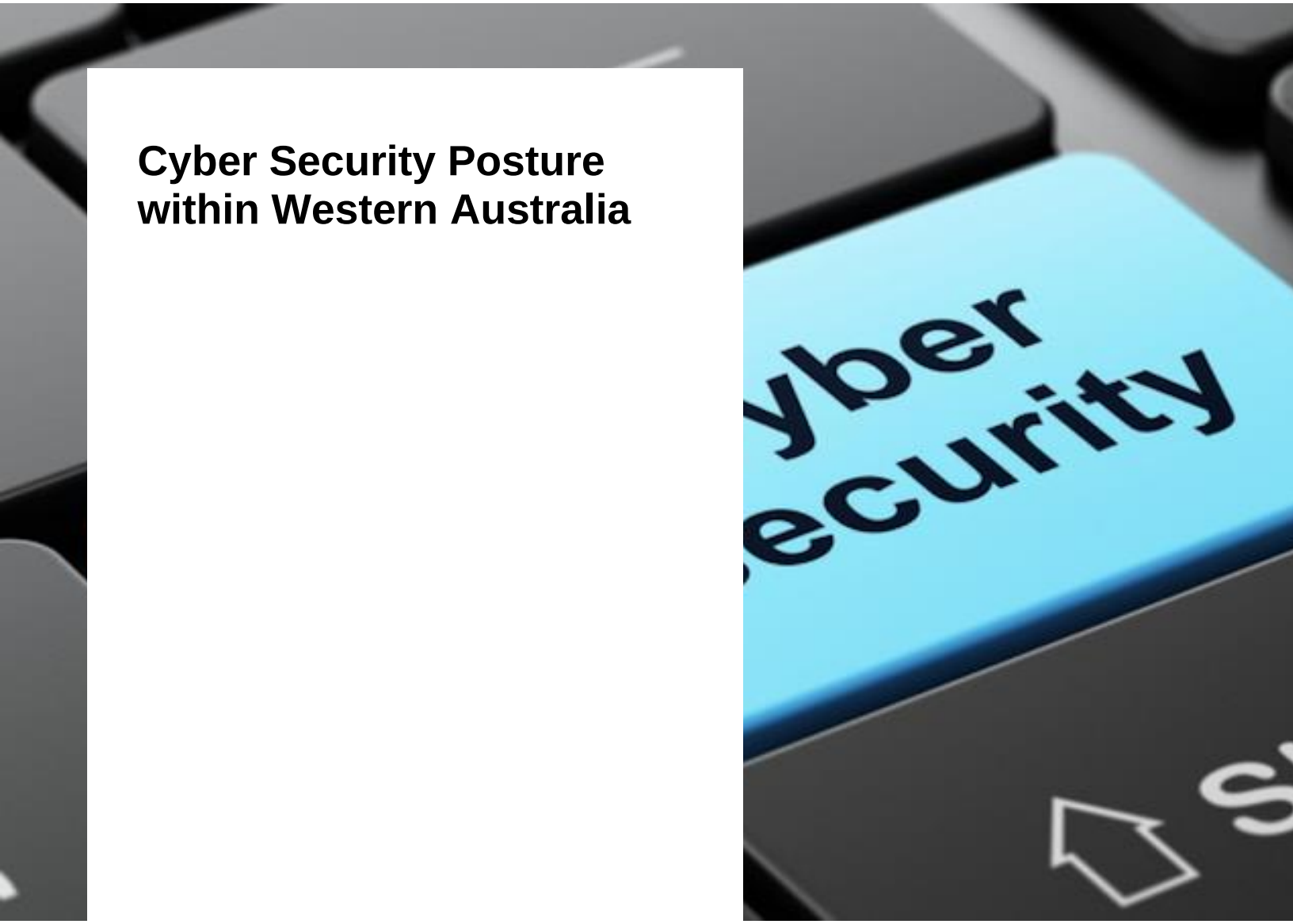
# Cyber Security Posture within Western Australia




**10 SEPTEMBER 2019**

**Terrene Global**

**Authored by: Brenda van Rensburg**

Terrene Global

## Table contents

## Executive Summary

Cybercrime is affecting Western Australia significantly and has already cost Australia over $1 billion in 2018.[1] According to ScamWatch,[2] Western Australia lost over $10 million from scams alone, during this time. This number was only based on those reported.

Western Australia has the highest percentage of small business owners in Australia, which make up 97% of all WA businesses. There are 147,168 single operator businesses in Western Australia that contribute over $48 billion to the State's economy[3]. According to the McGowan State Government, Western Australia's gross revenue was just a little over $200 billion for 2017/2018.[4] Small businesses account for 25% of Western Australia's gross revenue.[5]

Austbrokers have stated that 22% of Australian businesses were impacted by **ransomware** and could not continue with business.[6] As a result, cybercrime would impact Western Australia's economy by roughly $10 billion and would have a catastrophic effect on the unemployment rate that would further add a significant burden to the economy and resources.

**"International cyber incidents have disrupted power grids, degraded public health and transport systems, and damaged physical infrastructure. These new threats, if realized….could threated physical safety, economic security and the continuity of government and its services " Minister Peter Dutton[7]**

[1] https://www.smh.com.au/politics/federal/increasing-cyber-crime-attacks-costing-up-to-1b-a-year-20180410-p4z8ui.html
[2] https://www.scamwatch.gov.au/about-scamwatch/scam-statistics?scamid=all&date=2017
[3] https://www.smallbusiness.wa.gov.au/about/small-business-sector/facts-and-statistics
[4] https://www.ourstatebudget.wa.gov.au/2019-20/fact-sheets/2019-20-fact-sheet-set.pdf
[5] ibid
[6] https://www.austbrokerscanberra.com.au/news/the-impact-of-cyber-attacks-on-small-business/
[7] https://www.theaustralian.com.au/nation/politics/dutton-to-warn-of-evolving-cyber-threat-to-transport-and-power/news-story/5a0fa5e6aee764d6f422d9081844e7fb

With cybercrime now at the heart of our community, we are challenged with ways to reduce the impact on our communities and business sector. This briefing will cover **5 Steps** to combat Cybercrime in Western Australia.

I. Sustainable Digital Society

II. Critical infrastructure and vital services

III. Legislation & Legal Responses

IV. Cyber Literate Society

V. Cyber Talent Pool and Skills Acquisition

***The intensity of Cyber Crime has increased.***
***Every person and business in Western Australia, that uses the digital landscape, is a target!***

With the growing intensity of cybercrime in Western Australia, we have the opportunity to tackle the problem head on and lead Australia due to our resourcefulness.

# I. Sustainable Digital Landscape

## a. Corporate Accountability

Many businesses lack responsibility for securing PIIs (Personal Identifiable Information). In 2015, Marriot Hotel lost over 500,000 PIIs to a data breach. Marriott stored the PII in a text format and the credit card information in a weak 128-bit encryption.[8] Recently, a hosting company stated that they store PIIs in SHA-1 algorithm. This protection mechanism is weak and has been found vulnerable to collision attacks".[9] It is recommended that PIIs should have a minimum of 256 AES (Advanced Encryption Standard), commonly used by banks.[10]

With the abundance of security options, businesses are still applying the bare minimal protection. In a recent study by ECU, it was found 64% of Western Australia lawyers use Public Wifi for work.[11] **The current Notifiable Data Base Regulations state that legally, businesses only need to show that they took 'reasonable steps' to secure their data,[12] and this can no longer be acceptable.**

## b. Corporate's Insufficient Understanding

Cybercrime is a topical subject; however, many businesses still feel that they will not be a victim to cybercrime. In a recent study by Sherpa Insurance, they found that most of their customers felt that cybercrime was not an Australian problem and believed that they never experienced a privacy breach,[13] but over 6 million Australian's were a victim of Cybercrime in 2016.

According to Mark Gorrie, Territory Manager, Norton Business Unit, too many people feel they are invincible and skip taking basic precautions to protect themselves,[14] such as changing password regularly. **There should be an urgency placed on educating organizations about basic cyber habits which will reduce the risk of cyber exploitation.**

[8] https://www.forbes.com/sites/thomasbrewster/2018/11/30/marriott-admits-hackers-stole-data-on-500-million-guests/
[9] https://threatpost.com/hostinger-data-breach-14m-passwords/147681/
[10] https://bestcompany.com/expense-management-software/blog/what-does-bank-level-encryption-really-mean
[11] https://www.ecu.edu.au/news/latest-news/2018/05/client-data-potentially-at-risk-due-to-lawyers-lack-of-cybersecurity
[12] https://www.business.gov.au/risk-management/cyber-security/protecting-your-customers-information
[13] https://sherpainsurance.com.au/cyber-crime-dont-worry-it-wont-happen-to-me/
[14] https://eftm.com/2018/02/1-3-australian-adults-fall-victim-cybercrime-2017-47191

**c. Inadequate Security Approach**

In 2016, the West Australian Parliament developed an Innovation Strategy with one of the goals to take ideas from discovery to commercialism.[15] According to David Ross of Business Insider, App developers have grown by 20% in the last two years.[16] Exports of computer and information services grew 30% in 2018.[17] Louis Cremen, from Hackernoon, stated that they found over 3 million apps that had security flaws.[18] Furthermore, with the average smart phone user having an average of 26 apps on their device,[19] places a further burden on mobile security. Apart from this factor, there are a large number of apps that allow actors to track and obtain personal information.[20] Unfortunately, there is very little security attention given to technology during the development phase. There is also very little transparency given to consumers about digital products or services. In the recent years, it became known that Facebook sold a large portion of its data to 3rd parties.[21] Many people signed up to Facebook's platform without ever reading the Terms & Conditions. Facebook changed its Terms & Conditions several time since its launch in 2004, with knowledge that many members will agree to these changes, ignoring the facts that their data was being used. In a recent article by Jeff Wells, grocery stores are using apps to track shoppers in their store.[22] The app developer, Progressive Grocer, stated that many customers were unaware that stores where using this technology.[23] The lack of attention to security and transparency by developers is placing the West Australian community at risk. This fundamental flaw put California on the map as the first state to introduce the "Internet of Things (IoT) Bill" which requires manufacturers to equip devices with reasonable security features.[24] Notably, a valiant stand to protecting the community from known cyber-attacks.

[15] http://www.parliament.wa.gov.au/publications/tabledpapers.nsf/displaypaper/3914841a31223b11af0b93b4482580650045371a/$file/4841.pdf

[16] https://www.businessinsider.com.au/app-developer-numbers-in-australia-have-grown-20-in-2-years-2019-4

[17] ibidhttps://www.devere-australia.com.au/news/Australia-boasts-a-booming-tech-sector

[18] https://hackernoon.com/lack-of-mobile-app-security-2017-how-to-succeed-as-a-red-shirt-without-even-dying-b87d78627efa

[19] https://www.pcworld.com/article/2068824/study-finds-most-mobile-apps-put-your-security-and-privacy-at-risk.html

[20] https://techcrunch.com/2019/03/25/android-users-security-and-privacy-at-risk-from-shadowy-ecosystem-of-pre-installed-software-study-warns/

[21] https://www.bbc.com/news/technology-46618582

[22] https://www.grocerydive.com/news/grocery--could-in-store-tracking-technology-change-the-layout-of-the-grocery-store/535322/

[23] Ibid

[24] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

## II. Critical infrastructure and vital services

### a. Lack of Community Cyber Protection

There is an increase of crime that not only targets businesses, but also individuals. ABC News reported that victims of cybercrime have little representation or support from the police.[25] According to one of the victims, "there has been absolutely no contact from any authority, whether it's the Federal Police, the cybersecurity taskforce or whatever."[26] Western Australia Police have also made it known that they do not handle cyber incidences. [27] In a recent cyber scam, and elderly citizen contacted Terrene Global for help. She stated that she went to the police in her neighborhood and all they did was give her a brochure on how to report an online crime. The Western Australian police have stated that 30% - 40% of Cybercrime offences are committed by International offended. [28] Notably, they have also that there is an increase in the volume of cybercrime, a large percentage of the crime is multijurisdictional, and there is a cost involved with cross border prosecutions.[29]

In 2018, the New South Wales Police set up their first cybercrime squad with the number of arrests almost doubling from the year before[30] Lastly, the public are rapidly losing confidence in ACORN (Australian Cybercrime Online Reporting Networking) with more than 75% of the users dissatisfied in the lackluster outcome.[31] With the onslaught of cybercrime in our community, there needs to be actionable and recognizable police protection for victims of cybercrime.

### b. Lack of Digital Security Visibility

With diminishing confidence with cybercrime reporting systems, such as ACORN, there is also very little representation in regard to help with victims of cybercrime. As mentioned earlier, victims of cybercrime are often referred to using an online portal for reporting an offence, using the very tool which they experienced the crime. Furthermore, there is no local support for checking digital devices for embedded malware after a cybercrime has been committed. As a result, cyber criminals have access to infected devices well after the incidence. According to key findings of the NSW Small Business Commissioner, 93% of businesses want a tool to help them manage cyber risk and 75% end up using their own initiative.[32] Under the current

[25] https://www.abc.net.au/news/2017-02-27/cybercrime-victims-on-their-own-as-police-fail-to-follow-cases/8306814
[26] ibid
[27] https://www.police.wa.gov.au/Crime/Fraud/How-to-Report-Fraud
[28] https://www.aph.gov.au/DocumentStore.ashx?id=38378d85-540f-4ae0-a979-6e786c89cd6a&subId=564418
[29] Ibid
[30] https://www.abc.net.au/news/2019-02-11/cybercrime-skyrockets-in-nsw-as-murders-and-robberies-fall/10776982
[31] https://www.cso.com.au/article/648345/acorn-users-disappointed-outcomes-buried-government-review-found/
[32] https://www.smallbusiness.nsw.gov.au/__data/assets/pdf_file/0003/134931/cyber-scare-full-report.pdf

grant scheme, however, small businesses can apply for a grant for a cyber health check by a CREST recognized provider. Unfortunately, the majority of the CREST providers are recognized as part of the Big 4 in Western Australia, and business may only receive a maximum of $2100.00.[33] There is no ongoing support, especially if vulnerabilities have been found. As more than 60% of business in Western Australia sole operators, many of these businesses do not have the resources, or knowledge, to patch up vulnerabilities once uncovered.

## III. Legislation and Legal Responsibilities

Recently, Hannah Valentine was given 240 hours of community service for selling false tickets, under false aliases, using online platforms such as Instagram and Gumtree.[34] Notably, if she applied the same tactic, and sold these tickets directly to people via a physical face to face measure, she may have been tried under the *Criminal Code Act Compilation Act 1913* (WA) and/or the *Copyright Act 1968* (Cth)[35] which may have resulted in up to 7 years imprisonment.

Examples of cybercrime are as follows:

- Computer Intrusions & Attacks
- Computer Malware
- Interception of Data
- Search & Seizure
- Online Fraud
- Online Stalking & Cyber Threats
- Identity Theft
- Infrastructure Security
- AI & Block Chain Technology

Currently, the only dedicated cyber legislation is for Interception of Data, *Telecommunications (Interception and Access) Western Australia Act* 1996 and online fraud of digital signatures, *Electronic Conveyancing Act WA* 2014.[36] Notably, there are sporadic sections found within a number of Acts that can be used towards some cybercrimes, however there is no dedicated cybercrime legislation. Ironically, State of Victoria and New South Wales have made major milestones by passing the Data Sharing Act (Vic) 2017 [37] and Data Sharing (Government

[33] https://www.grants.gov.au/?event=public.GO.show&GOUUID=D6E83046-D97A-960A-D151681E029D646B
[34] https://www.abc.net.au/news/2019-07-19/ticket-scammer-hannah-valentine-avoids-jail-over-facebook-sales/11321552
[35] https://www.legislation.gov.au/Details/C2019C00042
[36]https://www.legislation.wa.gov.au/legislation/prod/filestore.nsf/FileURL/mrdoc_41506.pdf/$FILE/Electronic%20Conveyancing%20Act%202014%20-%20%5B01-b0-01%5D.pdf?OpenElement
[37] https://www.vic.gov.au/sites/default/files/2019-03/Victorian-Data-Sharing-Act-2017-web-guidance.pdf

Sector) Act (NSW) 2015.[38] Queensland has also made some major inroads with their judicial system. Recently teenagers were convicted for cyber bullying, a challenging area for any court.[39]

## IV. Cyber Literate Society

There is insufficient cyber awareness at civic level. This, in turn, adds significant strain to businesses who are already struggling to keep up with the impact of attacks on their own systems. Cybercrime cost banks near $600 billion a year.[40] Forbes wrote that people are more willing to cancel dinner plans than their credit card.[41] In a recent report, it was found that 43% of adults admitted to having bad cyber hygiene.[42] In another survey conducted across 2000 individuals, 93% admitted to knowing the risks of using passwords across a number of platforms, with 59% stating that they did so in any case.[43]

Education within our community is another concern. Although one can find several cyber security workshops in Perth, most of these workshops are often left to the demise of individuals with little skill in this area. Sometimes, industries may exploit struggling cyber professionals in this area who have hopes to gain employment. [44]

Unfortunately, if nothing is done at civic level, cyber criminals will continue to exploit the less educated. According to Austbrokers, 22% of small businesses that are impacted by ransomware were unable to continue with business. [45] This, in turn, will impact Western Australia by $10 billion and thus have a significant impact on Western Australian resource. If 22% of business closed their doors, there will be an increase in unemployment rate; a reduction State revenue; an increase in the number of homelessness; an increase in the number of suicides and place a significant burden on State resources such as Medicare and Centrelink.

[38] https://www.legislation.nsw.gov.au
[39] https://www.abc.net.au/news/2018-04-05/cairns-girl-charged-for-using-snapchat-to-threaten-teen/9622698
[40] https://www.securitymagazine.com/articles/88710-cybercrime-cost-600-billion-and-targets-banks-first
[41] https://www.forbes.com/sites/stevemorgan/2016/01/24/how-consumers-lost-158-billion-to-cyber-crime-in-the-past-year-and-what-to-do-about-it/#7f551dc72b65
[42] https://staysafeonline.org/blog/us-adults-bad-online-habits/
[43] https://www.darkreading.com/informationweek-home/password-reuse-abounds-new-survey-shows/d/d-id/1331689
[44] https://www.linkedin.com/pulse/unemployable-brenda-van-rensburg-/
[45] https://www.austbrokerscanberra.com.au/news/the-impact-of-cyber-attacks-on-small-business/

## V. Cyber Talent Pool and Skills Acquisition

There are many educational institutions that are benefiting from the increase of cybercrime, by offering Cyber Security education.[46] Notably, there have been reports that share the notion that there is a significant cyber security skill shortage. [47] However, when one looks at the current job opportunities, there are very few jobs available for cyber security professionals in Western Australia. From a recent search for jobs in this sector on 09 September 2019 with the LinkedIn platform, there were only 32 jobs offered within Western Australia. Another factor preventing cyber security professional from obtaining a job is that many agencies seek industry certificates that often prove too costly for an individual to obtain.[48] One exam for one of these certificates cost over US$500.00.[49] This excludes the workshop which is often between $2500 and $4000.[50] Other courses that are skill focused, such as technical exploits, can cost an individual over US$6500 for a one week program.[51] It seems, cyber criminals, who need no qualified training, have the upper hand!

Furthermore, the realm of cyber security is a broad one and many businesses seek to employ one person with the assumption that this is all they need. [52] According to Cybersecurity Ventures, there are more than 50 jobs descriptions within the cybersecurity sector.[53] Unfortunately, because the lack of civic level knowledge within this area, recruiters often look for one person willing to do the job of many. It would be an unreasonable and unfair request a person who has spent months, if not years, doing the right thing by looking for ethical work opportunities.

## VI. Solution

The solution to reducing cybercrime involves taking action which includes all five areas mentioned in this brief.

**Sustainable Digital Society**

Businesses need to take ownership and responsibility of Data Security. They also need to be transparent about data breaches and have the willingness to help those impacted by the

[46] https://www.computerworld.com.au/article/650122/400-million-cost-australia-cyber-security-skills-shortage/
[47] https://www.forbes.com/sites/martenmickos/2019/06/19/the-cybersecurity-skills-gap-wont-be-solved-in-a-classroom/#5681e0ce1c30
[48] https://www.forbes.com/sites/martenmickos/2019/06/19/the-cybersecurity-skills-gap-wont-be-solved-in-a-classroom/#5681e0ce1c30
[49] http://www.isaca.org/CERTIFICATION/Pages/default.aspx
[50] https://www.theknowledgeacademy.com/au/courses/cism-training/cism-training/perth/
[51] https://www.sans.org/event/new-york-city-summer-2019/schedule/
[52] https://www.linkedin.com/pulse/unemployable-brenda-van-rensburg-/
[53] https://cybersecurityventures.com/50-cybersecurity-titles-that-every-job-seeker-should-know-about/

breach. In a recent UWA cyber incidence where 30 laptops were stolen, individuals were left to 'fend for themselves' when it came to protecting their PIIs. [54] Recently, a student contacted Terrene Global looking for assistance in dealing with PIIs obtained as a result of the breach. Everything, including passport and Centrelink information, was on the device leaving this student exposed to identity theft. UWA had only sent them a vague email, and they had to figure the rest out themselves.

Furthermore, there needs to be a continuous effort in helping businesses develop and handle incidences. The current Notifiable Database Regulation requires businesses, that fall within the requirements set out in the regulations, to lodge a report if there is a breach. There are many businesses within Western Australia that are not familiar with these regulations and unknowingly face hefty fines.

Sandbox testing and transparency of terms & conditions need to be the forefront of businesses within Western Australia. Sandbox testing helps app develops focus on security measures before releasing the product to the market. Transparency of terms & conditions allows users to have knowledge of the platform 'hidden agenda' before signing up. The GDPR has recently amended their regulations and require all sites to advise visitors that cookies are being used. Cookies are a form of code that collects data about a visitor and follows their online movement after the site has been closed.[55] Companies still have the right to use cookies as long as visitor know that they are doing so.

**Critical infrastructure and vital services**

There needs to be physical presence of a cyber response team to help individuals, and businesses, with cyber threats and incidences. It should be Social Policy. Much like New South Wales, cybersecurity units can help increase confidence within the public sector and to help the West Australian community deal with a platform which the government has encouraged them to use.

Cyber Security Police units will also have the capacity to handle with incidences immediately. Email attacks have recently impacted businesses. Some of the emails come with death threats. A cyber unit can stop these emails quickly with several known exploits that are currently being used for hacking exploits and tools. Tools which are taught in educational institutions and in private workshops, as mentioned in this briefing.

[54] https://www.itnews.com.au/news/thieves-steal-laptops-with-30-years-of-data-from-university-of-western-australia-528774
[55] https://gdpr.eu/cookies/

**Legislation & Legal Responses**

There is a significant gap between legislation and the development of technology that gives rise to cybercrime. The creation of a cyber legislation council will help Parliament with development of cyber legislation. This council will research and uncover current legislative gaps and help develop legislation accordingly. The Eu have already tackled the legal issue which attacks crime against information systems.[56] Cyber Council members will have applicable experience within cyber security and good understanding of Commonwealth and State Law.

Furthermore, as the Western Australian police have stated, there is a significant cost with cross border prosecution. Opening communications, and relations, between states and international actors, will help unify legislative framework that aid legal works to tackle cyber crime efficiently. [57]

**Cyber Literate Society**

The goal is to develop a digital security vision which the local community will support and endorse. This will aid in proactiveness to protect and defend our state and residence. In 2008, Estonia created a community cyber security awareness program and in 2018 they were able to report an improved level of cyber awareness where more than 75% of the country will be implementing better cyber habits by 2022.[58]

Furthermore, local government will need to invest in funding digital initiatives to educate the community with cyber skills by endorsing local skilled cyber educators to champion this initiative. This will, in turn, help struggling cyber security professionals with full time, or part time work keeping the ethical minded individuals fighting cybercrime instead of encouraging them to take advantage of a legislative loopholes on the darker side of the digital landscape.

**Cyber Talent Pool and Skills Acquisition**

The goal for local government would be to use local talent for the greater good of Western Australia. This can be achieved by encouraging the creation of a local cyber hub, allowing students and cyber security professionals to assist cyber police, facilitate business and local councils with cyber education, and become cyber security ambassadors to help restore faith in a diminishing confidence in our legal capabilities within the public sector.

[56] Republic of Estonia, Cyber Security Strategy, Tallinn 2008
[57] https://issuu.com/apsm/docs/acsm_issue_7_iwd_women_in_security_/66
[58] Republic of Estonia, Cyber Security Strategy 2019-2022, Tallinn 2018

Furthermore, local government should look at developing an educational funding scheme whereby cybersecurity professionals can increase their skills and acquire nationally recognized certification that will help them with acquiring jobs in a broad range sector. In short, we are creating a cyber defense reserve team which can be called upon in the event of major cyber warfare, especially on our main infrastructure such as water and energy.

**ABOUT TERRENE GLOBAL**

Terrene Global is recognized across various industries for cyber security education, cyber IQ & EQ awareness, and have delivered multiple presentations on a wide variety of cyber subjects. Since cyber breaches often occur unknowingly through employees, contractors, or other third parties, which makes it critical to consider the human factor when working to improve organization's security and reduce cyber risks.

**ABOUT BRENDA VAN RENSBURG**

Brenda is the head of cybersecurity education for Terrene Global for data and cyber safety. Her experience across a spectrum of industries from Legal, Financial to Resources has given her an in-depth knowledge of how to relate corporate governance, enterprise risk management and cyber & data security management to directors, C-level executives and all employees within organizations. She also enjoys the uniqueness of practical white hat hacking to find weaknesses within organizational systems for the protection of data. Her signature presentation is a practical hacking demonstration for executives

Brenda is an internationally recognized author and has published several cyber security articles across a broad range of industries. She is also a global keynote speaker and was invited to present at AUSEC2019, local councils and local businesses. She was also a Telstra Business Awards (WA) finalist 2017, a Stirling Council Judge Award winner, and was one of 4 international guests invited to NASA.