



Behind the Dot | Issue 11 | May 2017

THE FRONTLINE FIGHT AGAINST CYBER CRIME

How the Federal
Police are taking
down crims

SECURITY TRENDS AND PREDICTIONS FOR 2017

PROTECT YOURSELF
Security measures to ward
against malicious attacks



SECURING AUSTRALIA

The dedicated Minister and a \$230 million
plan to defend our digital economy



Protect your business from attack

Cybercrime is alive and well in today's online environment. Unauthorised access to your website could be disastrous for both your business and your clients. Protecting your .au domain name is a positive step towards peace of mind - Safeguard your .au domain today.



Visit www.aulockdown.com.au

Participating Registrars:



www.btdmagazine.com.au

Contributors

Publisher:

AusRegistry

Editor in Chief:

George Pongas

Managing Editor:

Maggie Whitnall

Creative Director:

Michelle O'Reilly

Contributors:

James Brown

Alison Coffa

Danita Goodwin

Helen Hollins

Adrian Kinderis

Sarah Moran

Patrick Myles

George Pongas

Maggie Whitnall

Data Analysis:

Penelope Green

Account Management and Circulation:

Courtney Fabian

Lucian Popaly

Subscription and advertising Enquiries:

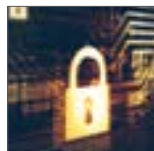
email: behindthedot@ausregistry.com.au

Features



Australian Federal Police fight against Cybercrime **9**

Taking down cyber crims from the frontline.



Securing Australia: The Federal Government's plan to keep Australians safe **13**

Our exclusive interview with the nation's first Cyber Security Minister.



Registry Security **11**

The security measures that can help protect domain names from malicious attacks, like .auLOCKDOWN and DNSSEC.

Departments



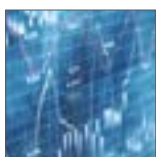
Under the Microscope **6**

A look at the strength of the .au brand and insights on which domain extensions Australians are buying.



Governance & Policy **19**

We meet auDA's new Director of Technology, Security and Strategy, Rachael Falk.



.au Research and Surveys **7**

Insights into attitudes toward security and trust online.



Channel Talk **21**

News and views from the .au retail channel. This edition: Do customers ask about online security products, or does it remain a hard sell?



Women in Technology **8**

Girl Geek Academy shares tips for parents to get girls into tech.



Glossary **22**

Abbreviations and definitions of key terms.

3,113,281

.au domain names

31 March 2017



Foreword



Welcome to the eleventh edition of *Behind the Dot*. Never before has the issue of cybersecurity been so front and centre in people's minds. It's hard to believe that it was just a little over a year ago that we released our previous edition of *Behind the Dot* dedicated to the important theme of security, and in that time, much has happened.

An unprecedented distributed denial of service (DDoS) attack on domain host Dynamic Network Services (Dyn) and the highly-publicised attack on the Australian Bureau of Statistics' website during the Census period, made 2016 arguably the most disrupted on record and many predict this is only the beginning. Neustar's Robin Schmitt gives his top four predictions of what we can expect to see in the online security space in 2017.

We were very fortunate to speak to the Minister responsible for overseeing the Federal Government's Cyber Security Strategy, Dan Tehan for our cover story. As the Minister Assisting the Prime Minister for Cyber Security, Minister Tehan has a big job on his hands when it comes to protecting Australian businesses and individuals from the scourge of cybercrime. Mr Tehan explains to us what every day Australians can do to help ensure we all continue to have access to a free and secure internet.

Traditional crimes such as fraud, scams and harassment are increasingly facilitated using technology, which are described as high-tech crimes, otherwise known as cybercrime. According to the Australian Government, cybercrime is impacting an increasing number of Australian businesses, putting many of them out of business within six months of an attack. It is estimated that this costs Australia's economy around \$1 billion each year. That's why in this issue, we take a look at what the Australian Federal Police (AFP) are doing at the frontline to combat serious and organised crime and protect Commonwealth interests from criminal activity in Australia and overseas.

We also look at the security measures that can help protect domain names from malicious attacks, and explore the concept of trust in our regular .au Survey and Research section. I trust you will enjoy our regular departments including Channel Talk and Governance and Policy, which all have explored online security and cybercrime.

I am pleased to present *Behind the Dot* magazine, and am hopeful it will serve to raise awareness of the real threat of cybercrime and encourage many of you to review your existing measures and address them if need be.

As always, we welcome your feedback and input on the magazine and thank you for reading.

A handwritten signature in black ink that reads "Adrian". The signature is fluid and cursive, with a long, sweeping underline.

Adrian Kinderis
CEO, AusRegistry



Under the microscope

By Patrick Myles – Net Knowledge

Measuring market share between different Top-Level Domains (TLDs) registered from within a country can give an impression of relative brand strength, awareness and relevance (studied over time it also helps determine changing buyer behaviour). So how many .au domains are registered from within Australia, and, what other domain extensions are being registered?

In the case of .au alone, most (around 97%) of the 3 million registered domains are registered from within Australia. There are, however, a similar number of domains under other extensions also registered within the country.

The chart shows the market share between locally registered .au domains and generic domains such as .com and .org. The data shows that .au has around 48% of the market – the rest is dominated principally by .com which has around 39% followed by other legacy gTLDs (.biz, net, .org) and a handful of new gTLDs (.sydney, .xyz, .melbourne etc).

It's important to note that these figures reflect the total volume of domains registered however does not consider *how* those domains are being used. For example, businesses may register names in both .au and a generic domain such as .com, however choose only one to host/promote their business from. In the advent of cross ownership we expect penetration is higher when brand protection is taken into account. Nonetheless, the volumes provide a good indication of the relative strength of the .au brand.

When comparing Australia (and .au) to other countries of comparable internet development, the market share is often very similar. The average across a sample of countries in the Asia Pacific region is around 48%, however, the range is wide with some countries dominated by .com and others with a strong preference to the local ccTLD. (Eg: .tw has 76% of the Taiwanese market).

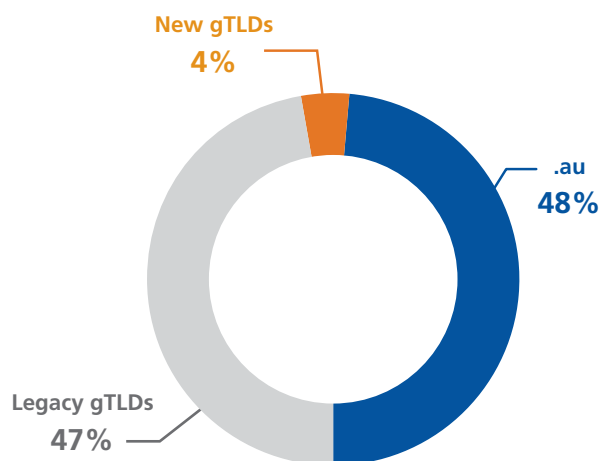
In terms of gTLDs, early indications in global trends suggest new gTLDs, although still with very small market shares are not impacting the ccTLDs greatly (at least in terms of volume). Geo-TLDs such as .melbourne, .london have the greatest affinity with ccTLDs and are progressing at a slow but steady rate and have shown to have some of the best renewal rates across all new gTLDs. ■

Note: Market Share estimates only include .au and recorded gTLDs (300) and does not include other ccTLDs registered from within Australia (such as .nz).

Data Sourced: Registrant distribution data sourced from AusRegistry (.au) and Zooknic (gTLDs).

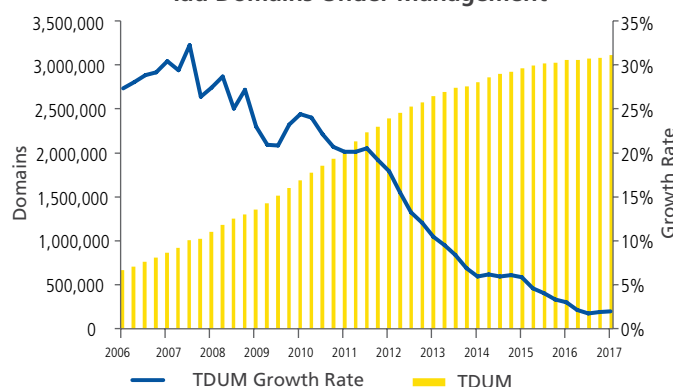
Australian TLD Market Share Est.

.au/gTLDs local registrations

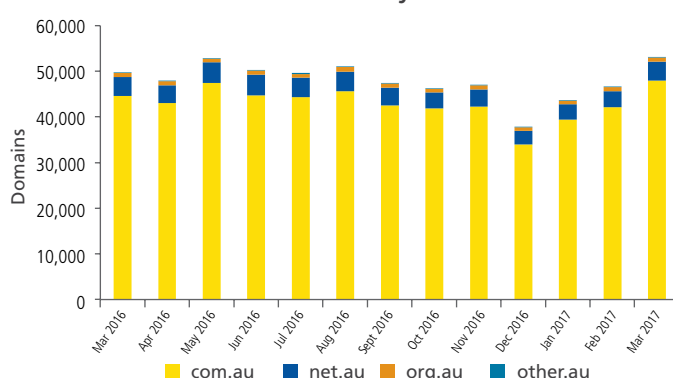


Source: Net Knowledge

.au Domains Under Management



.au Monthly Creates





.au research and surveys

By Penelope Green – Senior Data Analyst, AusRegistry

In November 2016, the annual .au survey findings were published in Edition 9 of *Behind the Dot*. Over the past four years the surveys have revealed much about domain name utilisation, user interaction and satisfaction with respects to the governance and operation of the namespace.

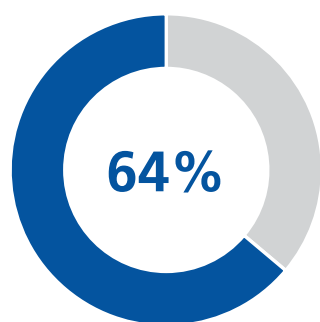
Several questions in this survey explored respondents' attitudes to security and trust online, asking what factors made them more likely to provide accurate personal information such as addresses or credit cards as a proxy for what factors engender trust. Encouragingly, 99% of the 3,011 survey respondents paid attention to security online. When asked what factors made them more likely to provide personal information to a website nearly three quarters (73%) responded with 'if it's a secure site' and nearly two thirds

(64%) with 'if it's an organisation I trust'. These responses illustrate a high awareness of security measures.

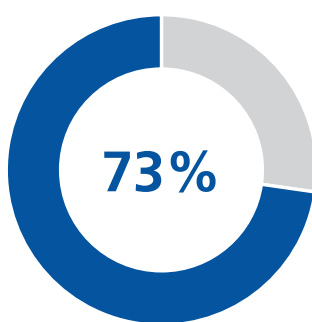
The survey also explored whether the zone of the domain made a difference. While zone was a secondary consideration to the characteristics of the individual site, it still made a difference to perceived trustworthiness. Well over half of all respondents (56%) are more likely to trust a website that ends with .au, with .com attracting just over a third of all respondents (36%) as more likely to be trusted. Whether this is nationalism (the survey targeted Australian residents) or a reflection of the history of effective policy and management in .au was not explored in depth, but this represents an opportunity for further research.

More detail can be seen in the charts below. ■

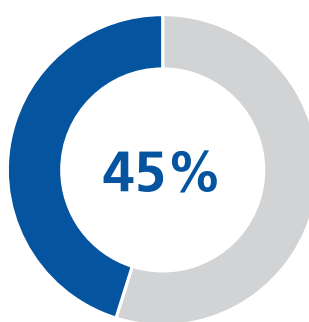
Website Characteristics Increasing Trust



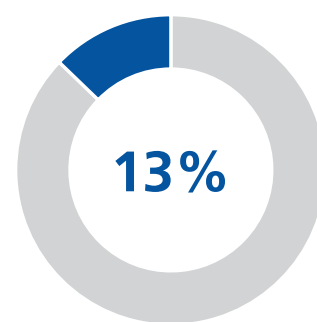
It's an organisation I trust



It's a secure site

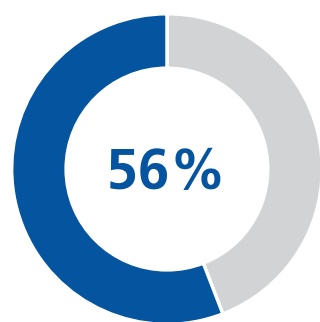


It's deemed secure by my security software

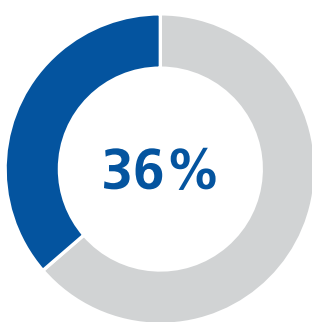


It looks professional

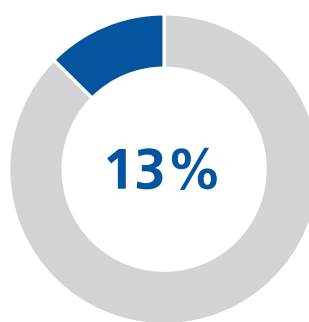
Website Zones Increasing Trust



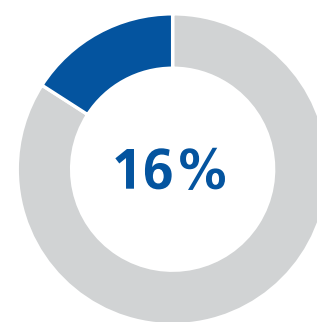
Trust: .au



Trust: .com



Trust: .secure



I don't pay attention



Women in Tech

By Sarah Moran – CEO of Girl Geek Academy

5 ways parents can get girls into tech

There is a huge urgency to place an emphasis on STEM education for young girls. The future of work is rapidly changing and the jobs of our children's future may not exist even today. Recent stats from the Australian Computer Society (ACS), reveal that females represent only 28 per cent of the ICT workforce (compared to 43 per cent in the wider workforce), and the rate of females enrolling in an IT degree has fallen from 8,627 in 2001 to 3,032 in 2013. By the time talented and high achieving girls reach the age of 15, most have dismissed the notion of pursuing an ICT career. For that reason, it's critical that we arm our girls with the technical skills necessary to, not only compete in the future jobs space, but to be leaders who have access to the same pay scale as their male equivalents. Here are my five tips for parents to get their girls into tech:

1

Start them young

I learnt to code when I was five years old – it wasn't any more difficult than another subject and I liked controlling what the computer did. I thought it was fun. When girls are younger, it's easier to engage them in technology before they have been exposed to any gender bias. 6-year-old girls already have gendered beliefs about intelligence and they're more likely to avoid games meant for "really, really smart" children. So it's also important to make sure you celebrate how fun it is to build things – it's fun to be a smart girl!

2

Teach yourself

There are so many workshops available for adults to learn to code that I would encourage parents to look into. Part of the challenge of getting girls (and children in general) into technology is the generation gap where some parents can assume it's "too difficult", when in reality it's so much easier than people think. By understanding how to build technology themselves, parents will be in the best position to support and guide their daughters, plus have a fun activity to do together – like the new bedtime story.

3

Embrace their creativity

Kids have the best imaginations and technology is basically built to a design brief. The process of getting from A to B is a creative process that involves design thinking and the ability to inject personality and originality into the technology creation. Provide them with the digital tools to let loose and watch them have fun while learning how to be the technology leaders of their future.



4

Embrace their femininity

Being a female in tech shouldn't mean having to assimilate into a "boys club" or environment. As much as the marketing for videogames and technology education is predominantly aimed at boys, it doesn't mean girls aren't welcome or won't enjoy the experience. We have to change this, and it starts with allowing our girls to build pink websites, if that's what they want, and at the same time encouraging them to be bold and play the "tough" games - that's what being a strong girl means. By simply allowing girls the freedom to build the technology that interests them, in the style and content that is personal to them, we will start to shift the needle back to an equal playing field where there is no right or wrong way to create technology.

5

It's important

We live on the internet and we're only going to spend more time in the digital world as we continue down the path of wearables, automation and robots. If this is the world we're heading into, and we're making a conscious effort to create gender equality, how can we leave the building of the internet in the hands of men? Currently, only 12 per cent of the internet is built by women, so we have a long way to go to ensure gender parity in this space. That's why the girls of today must be encouraged to contribute and take control of their future if they want to be true equals, fighting for the same leadership positions and pay as their male counterparts.

Sarah Moran is CEO of Girl Geek Academy, an organisation teaching 1 million women to get into tech and launch their own startups by 2025. Girl Geek Academy is a community for lifelong learning, following the whole journey of women in tech from age five to infinity.

AusRegistry teamed up with Girl Geek Academy to run its #MissMakesCode program in a Melbourne school - the first hackathon in the world created to build confidence and self-efficacy in the areas of algorithmic thinking, programming and coding for in young girls from 5-8 years of age. The full story will be available in the next edition of Behind the Dot. ■

Australian Federal Police fight against Cybercrime



By Maggie Whitnall –
Senior Client Services
Manager, AusRegistry

Times are changing with respect to how Australia is responding to the severity and frequency of cybercrime. In April 2016, Prime Minister Turnbull released Australia's Cyber Security Strategy¹, which aims to advance and protect Australia's interests online. More recently, the Senate passed the Privacy Amendment (Notifiable Data Breaches) Bill 2016 which, according to the Australian Privacy and Information Commissioner, Timothy Pilgrim, "...will strengthen the protections afforded to everyone's personal information, and will improve transparency in the way that the public and private sectors respond to serious data breaches²."

Since 2014, the Australian Cyber Security Centre (ACSC) has brought together cyber security capabilities across Defence, the Attorney-General's Department, the Australian Security Intelligence Organisation, the Australian Federal Police (AFP) and the Australian Crime Commission in a single location. The ACSC "is a hub for greater collaboration and information sharing with the private sector, state and territory governments, academia and international partners to combat the full range of cyber threats³".

Over time the AFP has seen the rising use and dependence on technology as one of the major influences on the domestic and international law enforcement operating environment. Traditional crimes such as fraud, scams and harassment are increasingly facilitated using technology, which are described as high-tech crimes, otherwise known as cybercrime.

The AFP is the Australian Government's primary policing agency responsible for combating serious and organised crime and protecting Commonwealth interests from criminal activity in Australia and overseas. The AFP's Cybercrime Investigation teams within the ACSC provide the AFP with the capability to undertake targeted intelligence and to investigate and refer matters for prosecution for those believed to have committed cybercrimes of national significance. The AFP is also the ACSC's conduit for State and Territory law enforcement. Ref: page 4, ACSC 2016 Threat Report, https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf

The AFP's Corporate Plan 2015-2019⁴ speaks to the continuously changing and complex environment in which they operate, largely led by globalisation and technology.

"Globalisation combined with the pervasiveness of internet-enabled communication, such as internet-enabled mobile devices, encrypted communication technology, mass communication and social media has changed the nature of policing. Cybercrime is a mainstay of criminal activity..."

...Australian computer networks (including the AFP's own systems) continue to be the target of cyber intrusion and attack. Criminal groups employ malware to obtain funds from financial service providers. Counter surveillance and encryption technology is now widely accessible and cheap, and private sector companies possess huge data sets which can assist law enforcement⁵."

So how do the Australian Federal Police fight cybercrime, and how successful are they?

In a 2015 paper entitled 'The Cybercrime Challenge⁶', Australian Federal Police Commissioner, Andrew Colvin wrote, "To be successful, law enforcement needs to be as innovative as its adversaries. Law enforcement must continue to adapt technologies,

increase and import skills and enhance partnerships—but it must do this at a much faster rate than currently occurs."

There are challenges however. The paper goes on to outline three main reasons why the "transnational nature of cybercrime creates difficulties for law enforcement" which include poor information exchange and cooperation between law enforcement agencies in different countries, a perpetrator's country not being equipped to conduct a suitable investigation and the country in which the culprit is located may have insufficient legislation or legislation that's incompatible with that of the victim's country.

Whilst Australia is a signatory to the Convention on Cybercrime⁷, which remains the only intergovernmental treaty relating to cybercrime, it is not without limitations given a number of countries with some of the highest cybercrime rates in the world are not members, such as Russia, China, India and Brazil. The treaty's main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

Back at home, Dr Tobias Feakin, Australia's first Ambassador for Cyber Affairs, has highlighted that law enforcement agencies must increase capabilities by investing in technology, building a sustainable skills base and building international partnerships⁸.

The \$230 million funding commitment announced as part of the April 2016 Cyber Security Strategy will partly be used to increase the number of

Between July 2015 and June 2016, CERT Australia responded to 14,804 cyber security incidents affecting Australian businesses, 418 of which involved systems of national interest (SNI) and critical infrastructure (CI). Ref: page 14, ACSC 2016 Threat Report, https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf

1 <https://cybersecuritystrategy.dpmc.gov.au/assets/pdfs/dpmc-cyber-strategy.pdf>

2 <https://oaic.gov.au/media-and-speeches/statements/mandatory-data-breach-notification>

3 <https://www.acsc.gov.au/about.html>

4 <https://www.afp.gov.au/sites/default/files/HTML/Publications/AFP%20Corporate%20Plan%202015-2019/index.html>

5 <https://www.afp.gov.au/sites/default/files/HTML/Publications/AFP%20Corporate%20Plan%202015-2019/index.html>

6 https://www.aspi.org.au/publications/underground-web-the-cybercrime-challenge/SR77_Underground_web_cybercrime.pdf

7 <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>

8 https://www.aspi.org.au/publications/underground-web-the-cybercrime-challenge/SR77_Underground_web_cybercrime.pdf

"The biggest threat to Australia is public ignorance – and this includes parents who pay insufficient attention to their children using home computers and smartphones."

Commander David McLean,
Manager Cybercrime Operations
Australian Federal Police



specialists conducting threat detection and awareness, technical analysis and forensic assessments of cybercrime in the Australian Crime Commission and the Australian Federal Police. According to the Guardian's Paul Karp, "It is estimated 101 more cyber security experts will be hired across the government and its agencies, about half of whom will be officers in the two crime-fighting agencies. The Federal Police will get a further \$20.4 million and the crime commission \$16 million to conduct threat detection, technical analysis and forensic assessment⁹."

The Australian Federal Police are actively engaged in investigating and in some instances prosecuting offenders against 'high-tech crime' which includes computer intrusions (any unauthorised access of a computer or network of computers e.g. malicious hacking), unauthorised modification of data, including destruction of data,

distributed denial of service (DDoS) attacks using botnets and the creation and distribution of malicious software (e.g. malware, viruses, worms and trojans).

In many instances, where an offence has occurred, Australian law enforcement will not have the authority to take action unless the matter falls within the jurisdiction of the Australian police i.e. with respect to a denial of service instance, the system or computer server where the content is hosted must be in Australia, or the offender causing the intrusion, disruption or impairment must be an Australian citizen. Hence the importance of international partnerships.

In many respects, education forms a large part of combating cybercrime. In an interview with Acuity Magazine (Nov 2016), Commander David McLean, Manager Cybercrime Operations, Australian Federal Police spoke about the challenges for law enforcement agencies in educating the public on the need to be vigilant and pro-active. The biggest threat to Australia, McLean says, is public ignorance — and this includes parents who pay insufficient attention to their children using home computers and smartphones. He said, "Our economy is only going to be expanding into increasingly sophisticated sectors and the vectors for attack are only going to increase¹⁰."

In an effort to address the education component of cybercrime, the AFP, along with Microsoft Australia, Datacom and the Commonwealth Bank of Australia have joined together with state and territory police and Neighbourhood Watch Australasia to deliver the Australian ThinkUKnow¹¹ program. Launched in 2009, the ThinkUKnow cyber safety program is Australia's first and only nationally delivered crime prevention program.

The free presentations are delivered by state and territory police, Neighbourhood Watch Australasia and accredited volunteers from the Commonwealth Bank of Australia, Datacom and Microsoft.

The presentations cover topics such as social media reputation management, cyberbullying, 'sexting', online grooming, online gaming, inappropriate content, privacy management, identity theft, how to protect devices and how to report matters when things go wrong.

In the later part of 2017 the ACSC will move to a new location. As reported in the Canberra Times, the move will represent a proposed "\$38.8 million relocation and fitout of the ACSC to Defence-leased buildings at Brindabella Business Park near Canberra Airport. If approved, the centre's new headquarters would incorporate multiple security clearance levels, a mix of classified, unclassified and public meeting rooms, and space for a major expansion of its workforce to about 650, flagged in this year's Cyber Security Strategy¹²."

Australia's current focus on cyber security is unprecedented and represents a strong commitment towards providing a safe and secure online environment for all Australians. However as Clive Lines, Coordinator at the ACSC points out that, "In order to have a mature discussion in 2016, it is particularly important that we get the language right - calling every incident a 'hack' or 'attack' is not helpful for a proportionate understanding of the range of threats and only promotes sensationalism."¹³ ■

The ThinkUKnow Program in summary:

- through accredited AFP and industry volunteers, delivered more than 380 presentations to more than 10,000 parents, carers and teachers
- through state and territory police, delivered presentations to more than 150,000 school students
- increased its volunteer base to more than 600, expanding in rural and regional Australia.

Go to: www.thinkuknow.org.au

⁹ <https://www.theguardian.com/technology/2016/apr/21/australia-230m-fighting-cybercrime-50-extra-police.html>

¹⁰ <https://www.acuitymag.com/technology/cybercrime-and-law-enforcement>

¹¹ <https://www.afp.gov.au/what-we-do/campaigns/thinkuknow>

¹² <http://www.canberratimes.com.au/national/public-service/australian-cyber-security-centre-to-relocate-from-asio-headquarters-20161121-gsu3x0.html>

¹³ <https://www.acsc.gov.au/publications.html>



By George Pongas
Sr Director, Product Management, AusRegistry

REGISTRY SECURITY

A connected world has infinite possibilities. The connection you have with your customers online has never been as strong as it is today. Your company's website is not only a crucial piece of capital, but its assets often contain customer information that is invaluable to your business. Unfortunately, this information is also extremely valuable to cybercriminals – nasty hackers who won't think twice about taking your site down to make a few bucks.

According to the Australian Government, cybercrime affects nine out of 10 Australian businesses, putting many of them out of business within six months of an attack. Organisations or individuals seeking to cause disruption and damage to company website assets can use a variety of tactics to gain unauthorised access to domain names. From hacking the company network and gaining access to account usernames and passwords, to masquerading as an authorised contact and requesting changes – there are many strings to a cyber criminal's bow.

If you were to perform a quick straw poll and ask friends and family members if they had ever received an email from a 'trusted' source that didn't look quite right you could be confident that most would say 'yes'. In fact, you might even discover that your daughter, your husband or your hairdresser has fallen victim to one of the scams and clicked on a dodgy link.

This needn't be all doom and gloom however, especially if you're the proud owner of a .au domain name. Like any good yarn, this one has room for a hero, or two.

Registry locks

Registry locks are a security measure for domain names that provide an added level of security for domain name Registrants. It works by locking domain names at the Registry level. Changes are monitored through direct communication between the Registrar authorised contact and the Registry, by following a strict authentication process.

AusRegistry developed its own registry lock service called .auLOCKDOWN following high profile security incidents in Australia and other countries that in some instances led to the unauthorised access of domain names. Unauthorised access in many instances can lead to:

- Hacking the company network and gaining access to account usernames and passwords
- Direct targeting of the company's hosting services
- Direct targeting of the Registrar of record
- Social engineering, i.e. masquerading as an authorised contact and requesting changes

While recommended for all .au domain name holders, .auLOCKDOWN is principally aimed at Registrants with valuable and prominent websites with high traffic volumes and those looking to mitigate risk against fraudulent or accidental delegation changes.

According to NetNames'¹ Axia Harrison, "clients understand the value of their digital assets and therefore understand the threats such as domain hijacking and the need to protect themselves against this." Harrison goes on to say, "I find the main reasons clients choose to take up .auLOCKDOWN include both internal and external pressures and expectations that their digital properties must be secure and trusted."

NetNames' understanding of the benefits of .auLOCKDOWN make it easy to promote the service to their customers. "Reduced risk of disastrous consequences – the cost certainly outweighs the potential damage caused to a brand from a domain hijacking."

When it comes to
Registry security,
the old adage
'prevention is
better than cure'
rings true.

DNSSEC

Domain Name System Security Extensions (DNSSEC) is a technology that was developed to protect against DNS-based attacks and hijacks by digitally signing data so you can be more assured it is valid. In order to eliminate this form of vulnerability from the Internet, DNSSEC must be deployed at each step in the DNS lookup process from root zone to final domain name attesting to the validity of the address of the site you visit.

At the end of 2014, auDA, the .au Domain Administration deployed DNSSEC to the .au zone securing the authentication layer between the .au zone and the root (".") zone.

Whilst there are several layers to the authentication process it was an important step providing .au Registrants with an opportunity to enable DNSSEC on .au domain names (provided it is offered by their .au Registrar).

A recent report² from ICANN indicates that just over 90% of the current 1,528 TLDs have been signed.

VentralIP Australia were one of the first auDA ISS accredited registrars to offer DNSSEC across supported TLDs, including com.au and net.au.

Chief Technical and Development Officer Craig Marchant says customers are provided with access to this service via both its customer API and frontend platforms.

"The benefits of DNSSEC are well known within the web hosting industry, however those who represent large business and corporate bodies outside of ICT are not yet fully aware of the security risks which may be mitigated by the relatively simple process of implementing DNSSEC," he says.

"By being one of the first to support such a fantastic security measure, we were able to offer a service that was not yet readily available within the Australian market.

"Everybody within the ICT industry has a responsibility to not only implement but also support features of this nature that have the potential to improve the security of our customers and the web hosting industry as a whole."

Three-factor authentication

A domain name Registry requires a high degree of security due to the nature of the data it holds. Unauthorised access can lead to catastrophic events including the redirection or even deletion of websites.

The .au Registry applies three-factor authentication (3FA) to confirm the identity of its users, known as Registrars. 3FA is a multi-faceted form of identification that requires three different types of credentials typically taken from the categories of 'knowledge' e.g. users names, passwords and PIN numbers, 'possession' e.g. key-fobs and ID cards and 'inherence' e.g. retina and fingerprint scans.

In order to successfully connect (via EPP) to the .au domain name Registry, IP restrictions, valid SSL digital certificates and secure usernames and passwords are all used to verify a user's identity.

Multifactor authentication dramatically increases the security of any system. The likelihood of a perpetrator having access to all three types of a user's identification is minimal.

When it comes to Registry security, the old adage 'prevention is better than a cure' rings true. There are some simple steps you can take to increase your website assets' protection from nasty cybercriminals. With the combination of .auLOCKDOWN, DNSSEC and three-factor authentication, you can be confident that you have a high level of protection for your company and your clients. ■

¹ NetNames is a leading provider of corporate domain management and online brand protection services: www.netnames.com

² http://stats.research.icann.org/dns/tld_report



SECURING AUSTRALIA

How the Federal Government
plans to tackle the next frontier in
defending our digital economy



Greater number of cyber security incidents

Almost one million Australians were estimated to be victims of identity theft online in 2014. Over 9,500 cyber crimes were reported to the Australian Cybercrime Online Reporting Network in its first three months of operation. The Australian Signals Directorate responded to 37% more government cyber security incidents in 2014 compared to previous years.

Greater number of targets

The range of possible targets is expanding from computers and phones to other devices connected to the Internet of Things, such as cars, fridges and medical equipment. There will be at least 50 billion connected devices by 2020.

Greater sophistication

Cyber attacks are becoming more sophisticated and previously unseen malicious activity, including infections to the firmware of hard drives, can now leave almost no trace. This saw software developers taking an average of 59 days to roll out patches for software vulnerabilities in 2014, compared to just four days in 2013.



By **Danita Goodwin**
Communications Manager, AusRegistry

In January this year, Prime Minister Malcolm Turnbull warned all Australians to be concerned about the threat of a cyber-attack.¹ This came off the back of a number of heavily-publicised incidents, including, an unprecedented attack that affected high profile sites like Netflix, Twitter and PayPal, and closer to home, the now infamous #censusfail debacle that a government review² found was the result of four Distributed Denial of Service (DDoS) attacks. These attacks, considered to be avoidable, caused a 40-hour outage of the Australian Bureau of Statistics' website during the Census period and a never-before-seen prevalence of the term 'DDoS' in mainstream media. In 2016, everyday Australians, businesses and the government woke up to the imminent threat of cybercrime and the potential it has to impact our economy, our safety and our way of life.

A little over a year ago the Prime Minister launched the Federal Government's Cyber Security Strategy. The Strategy sets out the Government's plan to improve Australia's cyber security – enabling innovation, growth and prosperity and establishes five themes of action for Australia's cyber security over four years. These themes are around a national cyber partnership, strong cyber defences, global

responsibility and influence, growth and innovation and a cyber smart nation.³ This is the first time an Australian Government has released a cyber security strategy and put real money behind it – to the tune of \$230 million.

In another first, a Minister Assisting the Prime Minister on Cyber Security was

Australians are
very early adopters
of technology...
what we've now
got to encourage
is early adoption of
security measures.

also appointed to oversee the Strategy's implementation. Minister Dan Tehan has tackled this role head-on, determined to ensure the community is aware of the threat of cybercrime and working together to stare these criminals down. With a strong background in trade, small business and international affairs, Minister Tehan knows all too well how the Internet, and technology more generally, have brought about great opportunity for Australia's prosperity. He is also acutely aware of the fact that with this opportunity comes newfound perils that must be overcome.

"There is nothing more important to our future prosperity than an open, free and secure internet," Mr Tehan says.

"The majority of Australians use the internet every day, whether it be running their businesses, paying their bills or keeping in contact with friends, so we have to ensure their ability to do that remains intact.

"It is also vitally important for our national security as well – cyber espionage is alive and well, and cybercrime is growing and every day, people are looking to use malicious means to exploit the Internet.

"We have to make sure it is secure and people have confidence and trust in using this important mechanism safely."

While this is an admirable goal, new threats arise almost every day and a good-looking document isn't going to achieve anything if it isn't understood, supported and adopted by all sectors of the community. According to Minister Tehan, this is the Government's biggest challenge.

"First we need everyone working together to *understand* the threat, and continue to work together to defeat the threat," he says.

"No one can give a 100 per cent guarantee that they are cyber secure, but understanding this and knowing that if government, industry and individuals work together we can make sure we're doing everything we can to keep ourselves safe.

"That is the best protection that we have."

1 <http://www.theaustralian.com.au/business/technology/major-ddos-attack-on-dyn-knocks-out-twitter-spotify/news-story/12e86c2ec7145bf77b1146480403bb>

2 <http://parinfo.aph.gov.au>

3 <http://cybersecuritystrategy.dpmc.gov.au>

According to PwC's *Global State of Information Security Survey 2016*, incidences of cyber-security breaches within Australia were the highest worldwide increasing by 109 per cent between 2015 and 2016.⁴ The government's Cyber Security Strategy reports that cybercrime costs Australia's economy around \$1 billion each year.

"Australia is a target because people see an opportunity," Mr Tehan says.

"An example I often give is in my local community, an accounting firm was hit

The basic point here is if you stand still in this area, you're going backwards.

by ransomware and it ended up costing \$10,000 to get the systems unfrozen.

"They were threatened with having all the information of their local clients released publicly which would have done enormous reputational damage to this small business. That was a \$10,000 hit to a local community and if it was the local bank that had been robbed then it would have been front page of the local newspaper for days.

"Instead this went uncommented on or unnoticed. Sadly because of the success that these criminals had with this local business, then it might embolden them to try it with another business in the town.

"The prevalence of this and how it is affecting our communities is sadly a lot more common than we imagine."

⁴ <http://www.pwc.com.au/consulting/assets/global-information-security/gsis-infographic-2016.pdf>

Education seems to play a key part in the Cyber Security Strategy, with almost \$15 million in funding for awareness campaigns and academic centres of cyber security excellence and programs to increase numbers of cyber security professionals in Australia.

"What we need to do is understand there are some basic steps you can take as an individual or as a business to ensure your 'cyber hygiene' or your cyber security is as well protected as it possibly can be," Mr Tehan says.

"This is what the government is doing through its Cyber Security Strategy and rolling out information through initiatives like 'Stay Safe Online Week' and the Stay Smart Online website, which provides resources available for businesses to learn how to be cyber safe.

"The more we can educate our children as well about how important it is to be safe online, the more it will become part of everything they do as they grow up.

"Make sure you talk with your children about the dangers that are out there. Then talk to them about what measures they can take, for instance ensuring they have proper passwords in place and they update those passwords.

"Ensure that when friends or family click on links they know what the link is. If they see emails or messages that are doubtful, don't automatically click on them. This is about awareness and capability building about the threat that's there and also the simple steps people can take to protect themselves."

While this may all sound fairly simple, what has become clear is many Australians don't realise the consequences of some of these actions.

What's more evident is that the growing reliance on technology and the internet means that the payoff for criminals is growing exponentially. The data that's online containing sensitive information

There is nothing more important to our future prosperity than an open, free and secure internet.

is seen as a gold mine for those with a malicious agenda.

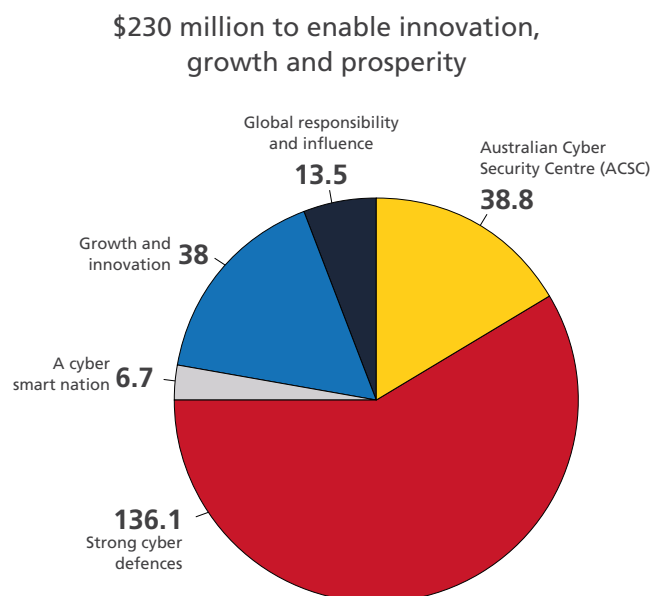
"What we've got to understand is Australians are very early adopters of technology and so therefore, we've been very early adopters of everything to do with the internet. What we've now got to encourage is early adoption of security measures," Mr Tehan says.

Minister Tehan knows that cyber security is an area that will continue to present challenges for the government, the business sector and individuals. But he says the key to this is remaining nimble and responsive, and why the government is determined to work with businesses to create opportunities for Australia to lead innovation in this space.

"The Cyber Security Strategy is a very good first step, but it's clear that we are going to have to continue to update it and look at ways to adapt the strategy to deal with the growing threat, because its changing nature and the technology changes means the threat continues to evolve. The basic point here is if you stand still in this area, you're going backwards." ■



Minister Assisting the Prime Minister on cyber security, Dan Tehan



MEMBER BENEFITS

**AUSTRALIANS VIEW .au AS A TRUSTED SPACE
ON THE INTERNET. IF YOU CARE ABOUT THE
INTERNET IN AUSTRALIA, BECOME A MEMBER**

auDA MEMBERSHIP BENEFITS:

- A VOICE IN THE FUTURE OF .au
- VOTE IN auDA BOARD ELECTIONS
- FREE ENTRY TO AUIGF
- INVITATIONS TO SPECIAL EVENTS
- QUARTERLY MEMBERS' NEWSLETTER
- AND MORE...

www.auda.org.au/Membership



...

**BECOME AN
auDA MEMBER
TODAY & HAVE
YOUR SAY**



Governance & policy

By **Helen Hollins** – General Manager Communications, auDA

Not only did the past year see a greater focus on encouraging women into the tech and security sectors, it has seen encouraging change at auDA – not least of all the introduction of an all-female executive team, appointed under new CEO Cameron Boardman.

One of those new female leaders, is Rachael Falk. Rachael took up the role as Director of Technology, Security and Strategy, in October 2016 and was tasked with providing strategic guidance and advice on cyber security, for auDA. She takes responsibility for ensuring that the .au online environment is safe and trusted. Rachael is collaborating with other key industry advisors on how auDA can become more proactive in the cyber security ecosystem. Rachael also has significant interaction with a range of government, industry, and academic stakeholders, to help shape that pathway.

Stepping back a bit, Rachael took a different, non-traditional road to her security and tech-focused career, initially studying law at University of Technology, Sydney. Upon admission as a lawyer, Rachael practiced in leading law firms both in Australia and overseas, most notably the magic circle firm Freshfields Bruckhaus Deringer in London (Rachael assures the author, no special dance or induction is required for entry to the magic circle, just hard work and smarts). Rachael, in the reverse of the brain drain culture of the day, returned to the land of milk and honey, spending ten years as a lawyer for Telstra. Most notably, she provided strategic advice and successfully managed a range of particularly sensitive and high profile litigation matters.

During part of her life as a lawyer, she was seconded to Telstra's Corporate Affairs group to act as a legal

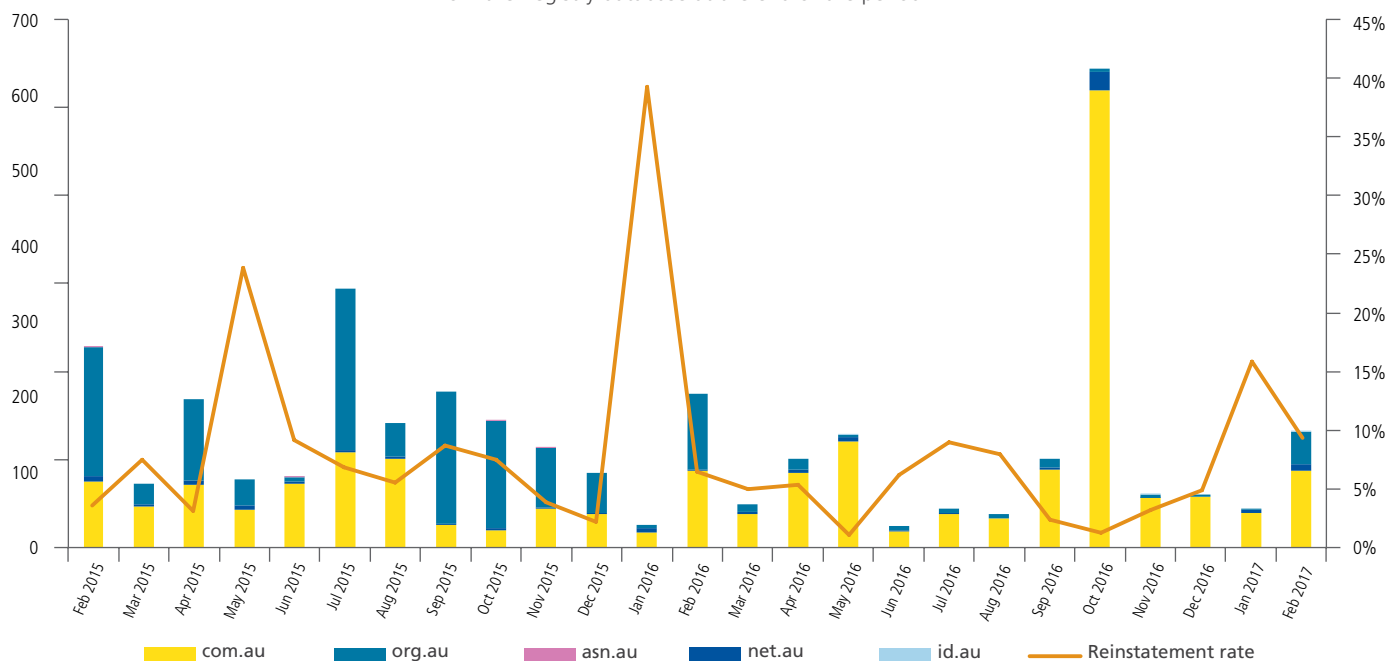
spokesperson. In that role, Rachael developed media strategies, provided guidance and engaged with the media while matters were before the Court. Given the strict nature of media reporting while matters are before the Court, and Rachael's experience with sensitive, high profile litigation, she was well placed to provide guidance that ensured appropriate media coverage and focus. This drew her to the attention of the Security Operations team at Telstra, which led to her role within Telstra's Cyber Influence Group. Sitting within Telstra's Security Operations Group, the first dedicated team of its kind within Telstra, they established and drove a cyber security culture within the company.

From this experience, Rachael co-developed the *Five Knows of Cyber Security*, an easy and accessible approach to cyber security that can be effectively used to manage cyber security risk from the Board down. Rachael continues as a presenter on cyber security and risk for ANU's National Security College Executive and Professional Development Program, where she gained her Master of National Security Policy (Advanced) with Honours.

Rachael is the perfect antidote for a male dominated sector, not afraid to call out conference organisers or employers alike for any gender bias she witnesses. She stands as a role model for many girls and women across sectors, with her genuine desire and dedication to encourage other women to think laterally when it comes to their future. Rachael brings a rare talent for looking at security in a different way, simplifying it and most importantly, helping bring other women with her. As Sheryl Sandberg might say, by 'leaning in'. Keep a look out for some big plans coming to life at auDA, under Rachael's leadership. ■

.au Policy Deletes (and Reinstatement Rate)

When auDA or the Registrar of record deletes a domain name for breach of policy, the domain name is placed into "pending policy delete" status for 14 calendar days. The domain name can be reinstated during this period, if the registrant is able to correct their breach of policy. If not, then the domain name is purged from the Registry database at the end of the period.



An aerial photograph of a city street grid, likely New York City, showing buildings, streets, and some green spaces. A large green rectangular overlay is positioned in the upper left quadrant, containing white text. The left side of the image is partially covered by a white grid pattern.

The Connected World Is Here. How's Your Security?

Products and services. Communications and commerce. You are connected to the world and the world is connected to you. This creates unprecedented opportunities at the price of bringing new risks. As the leader in Connection Science, Neustar knows what it means and what it takes to guard your business. We can help you make the decisions that empower you to safely and confidently connect people, places, and things so you can build a smart and secure connected customer experience.

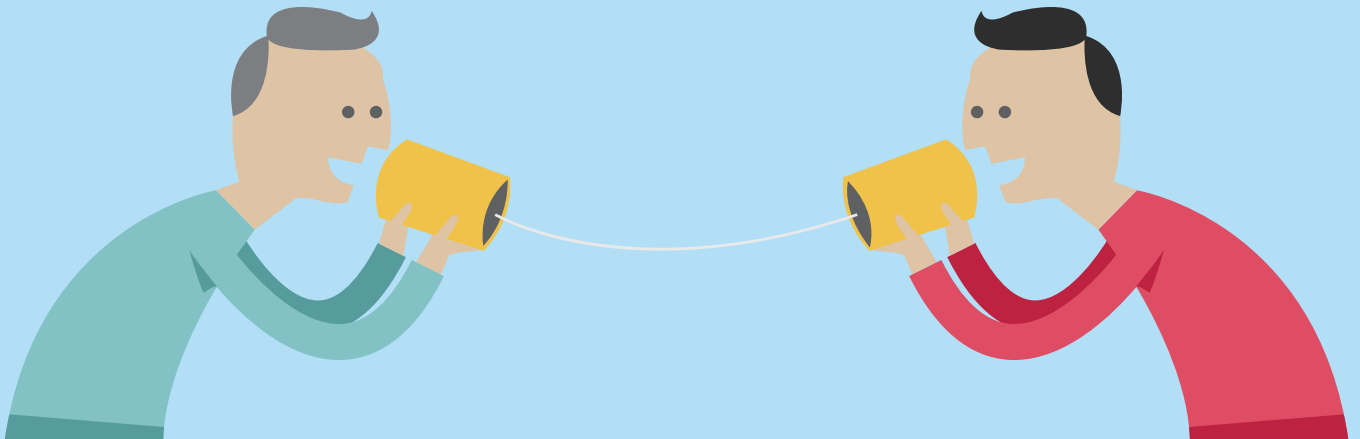
www.neustar.biz/brief

©2016 Neustar, Inc. All rights reserved.

neustar[®]

Channel talk

“ Do customers ask about online security products, or does it remain a hard sell? ”



LUCAS HIMSCHOOT

Instra.com

We've noticed more interest in security products as customers become more aware of increasing risks and threats to their online presence.

Products such as SSL certificates have become an essential addition when purchasing a domain name. Google results now flag websites without SSL certificates and we believe it's our job to keep customers informed about such changes and provide the best security advice.

At Instra we speak our customers' language and work with them to ensure they invest in the right solutions for their business. Purchasing security products can be daunting for many organisations, so supporting customers with information lowers barriers and ensures they have the knowledge to make informed and considered decisions.

STEPHEN HAMPSON

GoHosting.com.au

The SME sector is our core target market and customers choose GoHosting to get expert advice and quality products for their I.T. needs. The common question we field is, "what do I need to look after my business?". They look to us as experts who understand their business requirements and can recommend the best solutions. Customers are often alarmed by the risks we uncover when we perform a risk assessment on their current I.T. environment. However, once aware of

the risks most will do what is required to reduce exposure.

So, in summary – security products are in no way a 'hard sell' for us because we find most SME clients are smart, risk averse, realistic and welcome product suggestions to reduce their security risk profile.

JONATHAN HORNE

Terrific.com.au

We really saw a tipping point late last year with customers taking their online security seriously – possibly related to the hacking scandal that plagued the US elections. Perhaps businesses started to appreciate if a political party could be hacked then their business were in even greater danger.

Many businesses start with a simple security solution like SiteGuard.com to alert them of possible malware and site vulnerabilities. It's amazing to think, while desktop anti-virus is common, most businesses have nothing to protect their websites. Troubling when you consider websites may process credit cards and store confidential customer data.

I predict we are on the cusp of an online security paradigm shift. It will not be long before small business owners understand and invest in online security as seriously as they do physical security.

CRAIG MARCHANT

VentralP.com.au

In our experience customers generally ask about online security products reactively not proactively. Unfortunately,

this usually means damage has already been done to their business and brand. In relation to domain names, not many customers take advantage of security products such as Registry Locks to reduce the risk of an unauthorised third party making DNS changes to your domain name without an out-of-band communication channel between your Registrar and the Registry. A Registry Lock generally requires the Registrar to pick up the phone and call the Registry before changes can be made to DNS. However, the challenge is not just securing domain names. Hosting services are a typical attack vector and maliciously modified shared hosting WordPress installations are a common occurrence. In our digital world, a business's website is as important as a physical shop front, so it's important to secure them where possible and keep the latest updates applied to mitigate risk.

My final tip, if your service provider's control panel has 2-factor Authentication – enable it! It's not a fool-proof, but it costs nothing, makes it harder for the bad guys and may save your business from harm. ■

Want to contribute to the next 'Channel Talk' feature?

Channel Talk compiled by Courtney Fabian and Lucian Popaly. To contribute to Channel Talk, please contact behindthedot@ausregistry.com.au.

Glossary

Abbreviations

ACSC

Australian Cyber Security Centre

APNIC

Asia-Pacific Network Information Centre

APTLD

Asia-Pacific Top Level Domain Association

auDA

.au Domain Administration

ccTLD

Country Code Top Level Domain

CERT Australia

Computer Emergency Response Team Australia

DDoS

Distributed Denial of Service

DNS

Domain Name System

DNSSEC

Domain Name System Security Extensions

EPP

Extensible Provisioning Protocol

gTLD

Generic Top level Domain

IANA

Internet Assigned Numbers Authority

ICANN

Internet Corporation for Assigned Names and Numbers

ICT

Information and Communications Technology

IDN

Internationalised Domain Name

IP

Internet Protocol

TDUM

Total Domains Under Management

TLD

Top-Level Domain

WHOIS

A combined phrase to denote 'who is'

Definitions

Asia-Pacific Top Level Domain Association (APTLD)

APTLD is an organisation for ccTLD registries in Asia-Pacific region. APTLD was originally established in 1998, and in 2003 legally established in Malaysia. APTLD works as the forum of information exchange regarding technological and operational issues of domain name registries in Asia-Pacific region.

.au Domain Administration (auDA)

The policy authority and industry self-regulatory body for the .au domain space.

.auLOCKDOWN

.auLOCKDOWN a security measure for .au domain names that provides an added level of security for domain name Registrants. Domain names are locked at the Registry level, and changes are only possible through direct communication between the Registrar authorised contact and the Registry, by following a strict authentication process.

AusRegistry

The Registry Operator for the open 2LDs (com.au, net.au, org.au, asn.au, and id.au); the community geographic 2LDs (act.au, nsw.au, nt.au, qld.au, sa.au, tas.au, vic.au and wa.au); and two closed 2LDs (edu.au and gov.au).

Australian Cyber Security Centre

The Australian Cyber Security Centre (ACSC) brings cyber security capabilities from across the Australian Government together into a single location. It is the hub for private and public sector collaboration and information-sharing to combat cyber security threats.

Country Code Top Level Domain (ccTLD)

A TLD that is used to represent a country or external territory. Some examples of ccTLDs are '.uk' for the United Kingdom, and '.au' for Australia.

Computer Emergency Response Team Australia (CERT Australia)

CERT Australia (the CERT) is the national computer emergency response team.

Distributed Denial of Service (DDoS)

Distributed Denial of Service is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.

Domain Name/Domain

An identification string that defines a realm of administrative autonomy, authority, or control on the Internet. Domain names are formed by the rules and procedures of the DNS. Any name registered in the DNS is a domain name.

Domain Name System (DNS)

A hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates easily memorised domain names to the numerical Internet Protocol (IP) addresses needed for the purpose of locating computer services and devices worldwide.

Domain Name System Security Extensions (DNSSEC)

Domain Name System Security Extensions (DNSSEC) is a security extension that facilitates the digital signing of Internet communications, helping to ensure the integrity and authenticity of transmitted data.

EPP

Extensible Provisioning Protocol is a flexible protocol designed for allocating objects within technical registries over the Internet.



Internationalised Domain Name (IDN)

A domain name that includes characters from scripts other than the 26 letters of the Latin alphabet (a–z). An IDN can contain Latin letters with diacritical marks, or may consist of characters from non-Latin scripts.

Internet Assigned Numbers Authority (IANA)

A department of ICANN, which oversees global Internet Protocol (IP) address allocation, autonomous system number allocation, root zone management in the DNS, media types, and other IP-related symbols and numbers.

Information and Communications Technology - ICT

ICT refers to technologies that provide access to information through telecommunications. It is similar to Information Technology (IT), but focuses primarily on communication technologies. This includes the Internet, wireless networks, cell phones, and other communication mediums.

Internet Corporation for Assigned Names and Numbers (ICANN)

The global DNS administrator, formed in 1998, is a non-profit public-benefit corporation with global participants dedicated to keeping the Internet secure, stable and interoperable. It promotes competition and develops policy on the Internet's unique identifiers.

Internet Protocol (IP) Address

An IP Address is the numerical address by which a location in the Internet is identified. Computers on the Internet use IP Addresses to route traffic and establish connections among themselves; people generally use the human-friendly names made possible by the Domain Name System.

Registrant

An entity or individual that holds a domain name licence.

Registrar

An entity that registers domain names for Registrants and in the case of the .au ccTLD, is accredited by auDA.

Registry

The registry comprises of a database of domain names registered in each 2LD and a public WHOIS service for looking up the identity of the registrant of a domain name.

Reseller

An entity appointed by accredited Registrars to increase the retail channel of .au domain names.

Second Level Domain (2LD)

The alphanumeric string before the dot and the TLD. AusRegistry is the Registry Operator for the open 2LDs (asn.au, com.au, id.au, net.au and org.au); the community geographic 2LDs (act.au, nsw.au, nt.au, qld.au, sa.au, tas.au, vic.au and wa.au); and two closed 2LDs (edu.au and gov.au).

WHOIS

WHOIS (a combined phrase to denote 'who is') is a query and response protocol that is standard within the Domain Name Industry for querying Registry databases to determine certain information about a particular Domain Name.

Total Domains Under Management (TDUM)

Total number of domain names registered in the namespace.

Zone

A portion of the namespace in the DNS for which administrative responsibility has been delegated.

Disclaimer

This report has been produced by AusRegistry and is only for the information of the particular person to whom it is provided (the Recipient). This report is subject to copyright and may contain privileged and/ or confidential information. As such, this report (or any part of it) may not be reproduced, distributed or published without the prior written consent of AusRegistry.

This report has been prepared and presented in good faith based on AusRegistry's own information and sources which are believed to be reliable. AusRegistry assume no responsibility for the accuracy, reliability or completeness of the information contained in this report (except to the extent that liability under statute cannot be excluded).

To the extent that AusRegistry may be liable, liability is limited at AusRegistry's option to replacing, repairing or supplying equivalent goods or paying the cost of replacing, repairing or acquiring equivalent, or, in the case of services, re-supplying or paying the cost of having such re-supplied.

© 2016, AusRegistry Pty Ltd.



ausregistry.com.au

