2014

ANZ ONLINE TRUST AUDIT & HONOUR ROLL

Audit of the Australia & New Zealand 150

Best Practices In:

- Domain, Brand & Consumer Protection
- Site, Server & Infrastructure Security
- Data Protection, Privacy & Transparency

OTA

Online Trust Alliance

Under Embargo Until Nov. 25 8 am AEST

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Australia / New Zealand (ANZ) Online Trust Audit and Honour Roll is a companion to OTA's annual Global Online Trust Audit Honour Roll released in June 2014. Leveraging OTA's methodology and composite scoring algorithms, this report evaluated the practices of 150 consumer facing sites in Australia and New Zealand (ANZ 150), for best practices in brand protection, server security and privacy practices. The selection of sites to the ANZ 150 was based on a combination of factors including consumer site traffic within Australia and New Zealand, prevalence of past brand jacking or phishing exploits and industry sector leadership.

The criteria used in the Honour Roll are highly relevant to the security and privacy practices companies must implement to maximise online trust, focusing on three major categories weighted equally:

- Domain, Brand & Consumer Protection
- Site, Server & Infrastructure Security
- Data Protection, Privacy & Transparency

Primary goals for the Honour Roll:

- To recognise companies demonstrating their commitment to online trust and consumer protection.
- Develop and promote vendor neutral best practices.
- Provide prescriptive tools and resources to aid companies to help enhance their security, data protection and privacy practices.
- Recognise sites for moving beyond a compliance mindset to stewardship.
- Advance meaningful and measurable self-regulatory initiatives.

OTA
Online Trust Alliance
ONLINE TRUST
HONOUR ROLL
2014

2014 Honour Roll Recipients
Overall 14% of the ANZ 150 qualified for the 2014 Honour Roll, with the following sites being named to the 2014 Honour Roll. This represents 17% of Australian and 8% of New Zealand sites qualifying.

AUSTRALIA 2014 HONOUR ROLL RECIPIENTS

Australian Taxation Office - Ato.gov.au
AVG Technologies - AVG.com
Catch of the Day - Catchoftheday.com.au
Commonwealth Bank - Commbank.com.au
Coles - Coles.com.au
David Jones - davidjones.com.au
Gumtree - Gumtree.com.au
JB Hi-Fi - Jbhifi.com.au
JP Morgan Chase - jpmorgan.com
Kogan - Kogan.com
New South Wales Government - Nsw.gov.au
Rio Tinto - Riotinto.com
The Age - Theage.com.au
The Sydney Morning Herald - Smh.com.au
True Local - Truelocal.com.au
Virgin Australia - Virginaustralia.com
Xero - Xero.com

NEW ZEALAND 2014 HONOUR ROLL RECIPIENTS

HealthPost - Healthpost.co.nz
New Zealand Post - Nzpost.co.nz
Trade Me - Trademe.co.nz
Xero - Xero.com

Comparing Australia and New Zealand, Australia outscored New Zealand in Honour Roll achievement by 9%. New Zealand lagged behind Australia in key areas including 20% points in brand and domain protection and 10% points in privacy and data sharing practices. Compared to the Global Honour Roll, the number of sites in the ANZ qualifying for the Honour Roll surprisingly lagged by 14% points.

75% of ANZ sites received a failing score in one or more areas indicating these sites may become targets for abuse, potential hacking and social engineered email spoofing. These findings serve as a call to action to complete security audits including their DNS, SSL and email security infrastructure. In subsequent analysis it appears many of the failing issues were operational oversights and mistakes, underscoring the need for vigilance and frequent operational reviews as opposed to the need for added security expenditures.

The privacy landscape and baseline security requirements are evolving as the definition of personally identifiable information (PII) is rapidly evolving and cybercriminals are constantly probing for vulnerabilities. Public policy and regulations are also evolving, applying to not only where an organisation may have a nexus, but more importantly to where their users and site visitors physically reside.

Governance, compliance and most importantly stewardship expands beyonds one's geographic boundaries. The responsibility of a site's security, protecting brands from spoofing and adopting consumer centric privacy polices does not rely on IT, or Chief Security or Chief Privacy Officers alone. All functional areas of an organisation have a shared responsibility and need to take a holistic view of security and privacy policies. Concurrently board members share a responsibility, and need to ask management key questions, starting with what data they collect, why are they are storing it and if they are adequately funding security initiatives balanced against their risk appetite.

As businesses throughout the world amass big data, they need to be prepared for the likelihood of a data breach or loss incident. All organisations small and large need to develop and continually update an incident response plan Such plans need to address prevention, detection, notification, remediation and recovery plans. Those that fail to do so are increasingly finding themselves and their Board open to legal risks and as importantly irreversible reputation harm. To assist business in the development of such plans, OTA has published a Breach Response Planning Guide reflecting input from stakeholders worldwide.[1]

[1] OTA Data Breach Readiness Guide & Resources https://otalliance.org/resources/data-breach-protection

METHODOLOGY & SCORING

The development of this report represents the Online Trust Alliance's (OTA's) commitment to open and transparent multi-stakeholder initiatives. A public call for comments was issued in November 2013 in parallel with meetings with trade organisations, consumer advocates and leaders in the private and public sectors. Feedback was directly solicited from the Australasia region reflecting input from social sites, ecommerce, domain registries and infrastructure providers.

The feedback and recommendations were incorporated into the methodology released in March 2014.[2] This process represents OTA's commitment to providing businesses prescriptive advice to optimise their security, brand protection, data and privacy practices. The 2014 Online Trust Audit includes a composite analysis focusing on three major categories:

- Domain, Brand & Consumer Protection
- Site, Server & Infrastructure Security
- Data Protection, Privacy & Transparency

Sites were eligible to receive 300 total base points, comprised of 100 points in each of three categories plus up to 30 total bonus points for implementing emerging best practices. As in previous years, the criteria were adjusted to address the constantly evolving threat environment and the need for all sites to continually monitor their security and privacy practices, in essence "raising the bar" for Honour Roll qualification. To qualify for the Honour Roll, sites had to receive a composite score of 80% or better ***and*** a score of at least 55% in each of the three main categories.

Data sampling specific for the ANZ 150 was completed between August 15 and September 1, 2014, following the Global Honour Roll Audit data sampling between April 15 and May 23, 2014. All analysis was done anonymously. As outlined in the Global Audit, a site's configuration or practices may have changed since the sampling and the data only reflects findings during this snapshot in time.

It is important to note that the breakdown or complexion of the type of sites within the Global Audit and ANZ 150 varies significantly and may contribute to the decline in average number of sites qualifying for the Honour Roll. The largest factor creating this imbalance was in part due to the Global Audit including the Internet Retailer 500, which represents the 500 largest ecommerce sites worldwide and comprised 69% of the Global sites sampled.

SAMPLING SEGMENTATION

	Australia 100	NZ 50	ANZ 150	Global 750
Ecommerce	36%	40%	37%	69%
Financial Services	23%	26%	24%	13%
Social /News / Media	23%	16%	21%	13%
Government	18%	18%	18%	7%

Figure 1 - Sample Segmentation

[2] The 2014 methodology is posted at https://otalliance.org/initiatives/2014-methodology.

SCORING CRITERIA

DOMAIN, BRAND & CONSUMER PROTECTION

- Email Authentication Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) - *part of the base score, maximised by implementing both methods at top-level and subdomains*
- Domain-based Message Authentication, Reporting & Conformance (DMARC) – *part of base score, increased weighting in 2014*
- Domain Locking – *penalty if domain not locked*

SITE, SERVER & INFRASTRUCTURE SECURITY

- Secure Sockets Layer (SSL) Server Configuration – *base score of 100, with increased granularity and requirement levels in 2014*
- Extended Validation SSL Certificates (EV SSL) – *bonus points*
- Testing for XSS, iframe exploits, malware, malicious links – *penalty if these threats exist (new in 2014)*
- Always On SSL (AOSSL) – *bonus points*
- Domain Name System Security Extension (DNSSEC) – *bonus points*

DATA PROTECTION, PRIVACY & TRANSPARENCY

- Privacy Policy – *part of base score*
- Third Party Tracking on Site – *part of base score*
- Layered Privacy Policy – *bonus points (new in 2014)*
- Do Not Track Privacy Policy Disclosure – *bonus points (new in 2014)*
- Honoring of Do Not Track Browser Settings (DNT) – *bonus points*
- Implementation of Tag or Privacy Management Systems – *bonus points (new in 2014)*
- Public vs. Private WHOIS registration – *penalty if private*
- Data Breach & Loss Incidents – *penalty if incident in last 2 years*

The factors are weighted and scored based on the impact they have on email safety, brand protection, website security, consumer transparency, and overall best practices that will distinguish an organisation and brand from a business and consumer perspective. Results are used to assess each organisation's qualifications for the OTA Honour Roll.

ANZ HONOUR ROLL HIGHLIGHTS

As shown in Figure 2, 14% of the ANZ sector qualified for the Honour Roll, lagging behind the Global segment by 12% or a decline of nearly 48%.

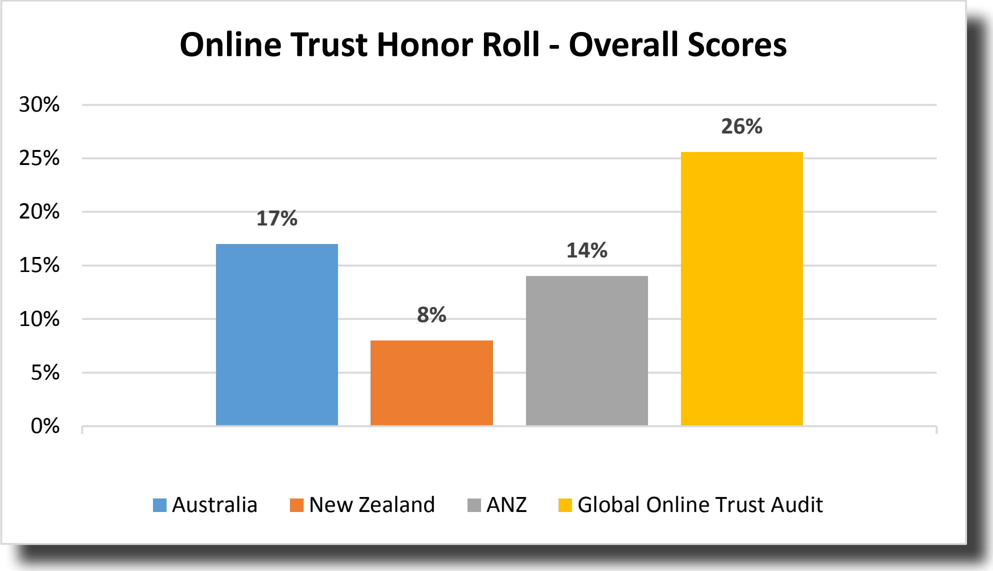

Figure 2 – Honour Roll Summary

Figure 3 provides a breakdown of the average of the three major components of the composite score: Brand & Domain Protection, Server Security & SSL Infrastructure and Privacy. The positive news is that the average site security / SSL scores sampled are consistent worldwide. The largest delta observed in the New Zealand sector was in the brand protection and privacy category.

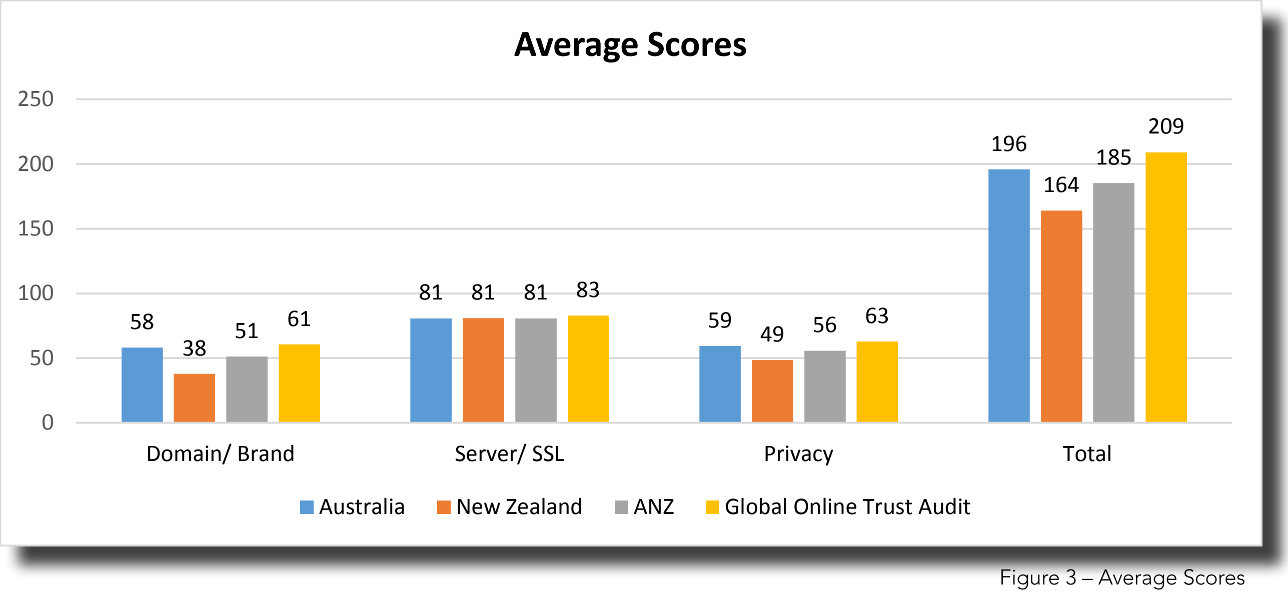

Figure 3 – Average Scores

FAILING GRADES

The Online Trust Audit also examines major shortcomings impacting consumer trust and reasons why organisations did not achieve Honour Roll status. Figure 4 shows the percentage of each segment that had a failing grade (<55%) in one or more of the three main categories. As noted, a single score below 55 in any of the three categories automatically disqualifies a site from the Honour Roll.

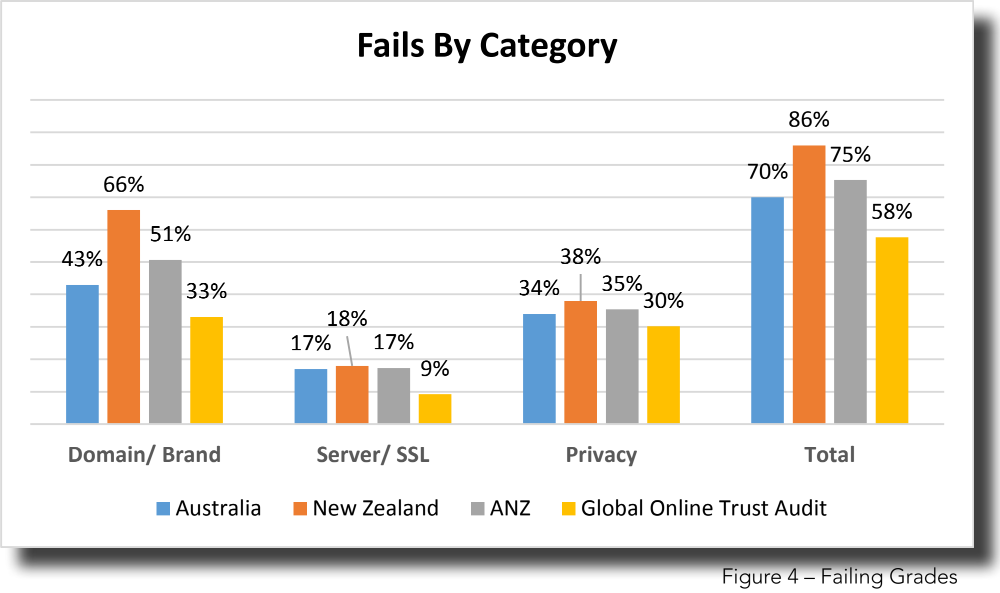

Figure 4 – Failing Grades

Domain & Brand Protection
Inadequate domain and brand protection was the primary cause for failures in all segments, highlighted by 66% of the NZ 50 receiving failing grades. The low scores were primarily based on the incomplete and inconsistent application email authentication support for SPF and DKIM at top-level domains. While marketers have been quick to adopt these protocols at the delegated sub-domain level, this offers little or no protection from the spoofing and malicious email purporting to come from the main corporate domains. A secondary cause for low scores is the lack of DMARC records. The increased occurrence of forged and deceptive malicious email, compounded by the ease with which this vulnerability can be discovered by cybercriminals, makes this an area of major concern for risk to brands and consumers.

Privacy Practices
Insufficient privacy practices constituted the next largest cause of failures, with one-third receiving failing scores, driven by inadequate disclosures addressing use, retention and data sharing. Other major causes of failing scores in this category were outdated privacy policies and use of website trackers that share information with other entities. While scored as bonus points, other contributing factors were the lack of layered privacy notices and "Do Not Track" disclosures. It is important to note these shortfalls can be remedied in a straightforward manner within the site's privacy policy and by re-evaluation of data sharing practices.

Site Security
Site security was the lowest cause of failure, showing that the vast majority of organisations across all sectors have implemented at least the minimum recommended level.

DOMAIN, BRAND & CONSUMER PROTECTION

EMAIL AUTHENTICATION

Email authentication technologies, namely Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM), help prevent phishing and spam and help protect consumers from receiving spoofed and forged email.[3] Email authentication allows senders to specify who is authorised to send email on their behalf. Building on email authentication protocols, DMARC adds a policy assertion providing receivers direction on how to handle messages that fail authentication. Domain locking ensures that domain ownership cannot be transferred without the owner's permission, further helping to protect a site's brand from abuse.

An accompanying report was published earlier this year providing in-depth review and discussion of email authentication.[4] This report includes a deep dive of DMARC, including an analysis of the adoption of reject or quarantine policies. Such policies are recommended to maximise brand and consumer protection by providing receiving networks and ISPs direction to reject or quarantine email which fails email authentication verification.[5] Best practices include:

- Implement both SPF and DKIM for top-level domains, "parked" domains (not used for email) and any major subdomains seen on websites or used for email.
- Implement DMARC for all appropriate domains, initially in "monitor" mode to receive feedback and verify accuracy of email authentication, and eventually to assert a "reject" or "quarantine" policy to receivers.
- Implement inbound email authentication and DMARC support to protect employees and corporate data from spear phishing exploits.
- Ensure that domains are locked to prevent domain takeovers.

Email authentication is the most significant factor which prevented ANZ sites from qualifying for the Honour Roll. Specifically, the NZ 50 adoption of both SPF and DKIM is nearly 50% below that of the general Global Honour Roll as outlined in Figure 5. As noted, SPF adoption is higher than DKIM adoption across all sectors, primarily due to its ease of implementation, whereas DKIM requires additional configuration and updates to outbound mail servers. Organisations worldwide have found that adoption of **both SPF and DKIM** best enables receivers to detect and block forged and malicious email, while reducing the risk of false positives from mail that is forwarded or sent from mailing lists.

Reviewing the subsegments of the ANZ 150, it is evident that online retailers and social platforms, which are most heavily reliant on email interaction with their users/customers, have recognised the value of email authentication. Conversely, increased efforts are needed by other sectors including government organisations to implement authentication at the top level domains.

[3] OTA Glossary https://otalliance.org/system/files/files/resource/documents/ota_glossary2014.pdf

[4] https://otalliance.org/EmailAudit

[5] https://otalliance.org/dmarc

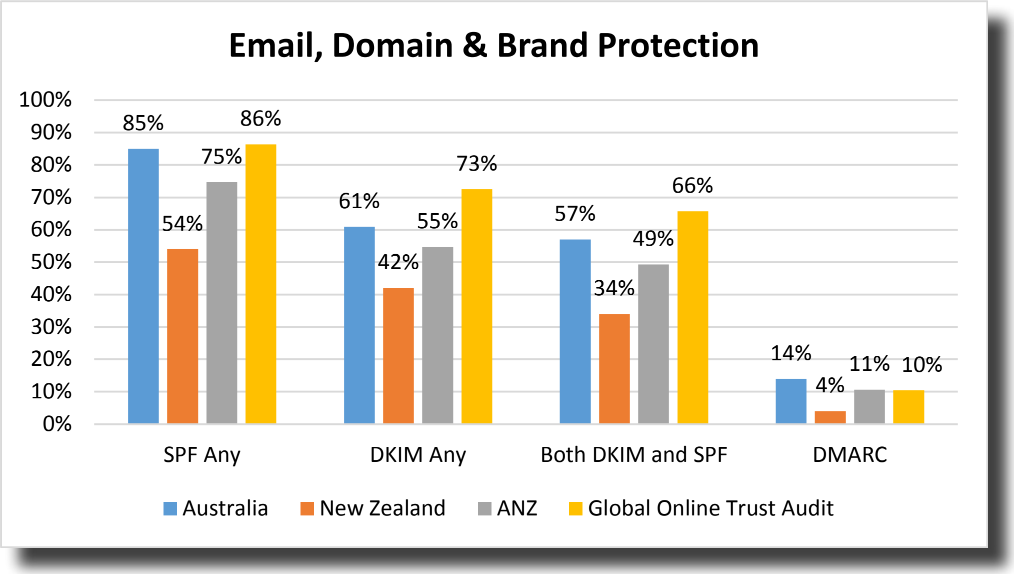

Figure 5 – Email Authentication Adoption

DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING & CONFORMANCE (DMARC)

Introduced in early 2012, DMARC provides significant benefits to the domain holder. DMARC leverages and relies on SPF and DKIM to provide reporting on how receivers process inbound email, reporting back to domain owners on incidents of forged or unauthenticated email. Most importantly DMARC provides a policy assertion for ISPs and corporate networks on how to handle unauthenticated email. Such assertions or policies provide receiving networks direction on when to reject or quarantine email failing authentication validation checks.

Implementation is easily accomplished by inserting simple text records in the DNS zone, with no server reconfiguration required. DMARC is now a baseline scoring component in the OTA Honour Roll with increased weighting since first added to the Honour Roll methodology last year. While worldwide adoption remains low, ANZ adoption is on par with other geographies sampled. All organisations are encouraged to publish their DMARC policy, built on the adoption of both SPF and DKIM on all parent and related subdomains.

As organisations complete an audit of their outbound email streams and DMARC reports they need to optimise their SPF records and DKIM signing practices. Once all outbound mail streams and domains are analysed and fully authenticated with both SPF and DKIM, it is recommended that organisations modify their DMARC record moving from a null or no reject policy, to a “reject or quarantine” policy. Doing so will help to maximise consumer protection from spoofed email.

SITE, SERVER & INFRASTRUCTURE SECURITY

A site's trustworthiness is primarily defined by the security of the infrastructure. Users want to know that they are on the right site and that their data transactions are secure. Proper implementation of best practices in this category also protects the site itself from attack.

In addition to a server's SSL optimisation, OTA advocates two best practices; 1) Extended Validation SSL Certificates, providing added validation of the identity of the web site and a trust indicator in the browser, and 2) Always On SSL (AOSSL) or SSL everywhere. AOSSL is a proven, practical security measure that should be implemented on all websites where users share or view sensitive information. AOSSL helps secure and encrypt the entire web session between the client device and server. AOSSL has gained broad adoption by leading banks, social sites including Facebook, LinkedIn and Twitter and search engines including Bing and Google.

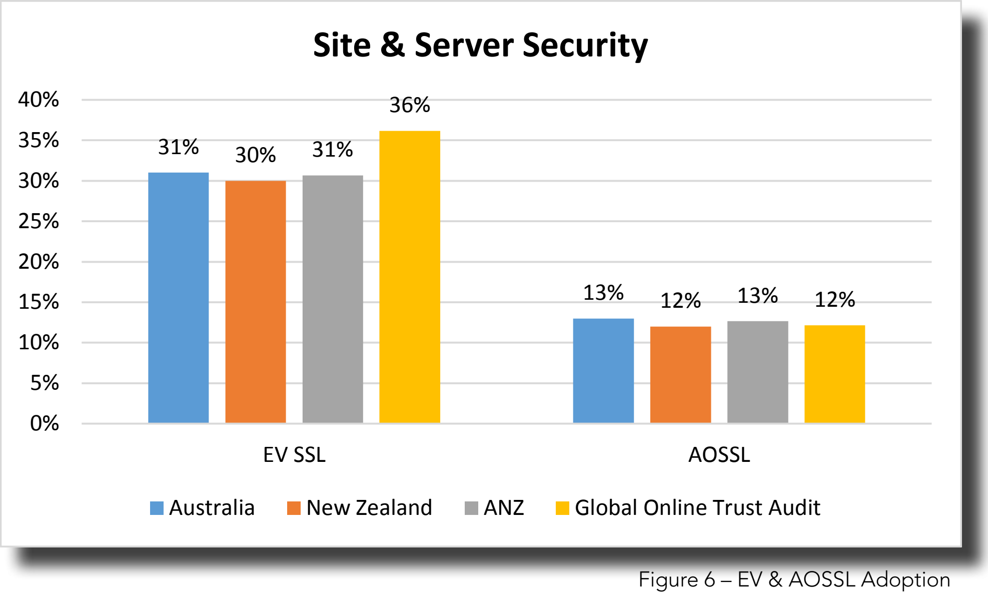

Figure 6 – EV & AOSSL Adoption

Best Practices

- Optimise SSL implementation using information gleaned from tools such as Qualys SSL Labs, with specific focus on vulnerabilities that earn a letter grade of "F".
- Use EV SSL on sites that are frequently spoofed and for sites where users need to be assured they are at a legitimate site.
- Implement AOSSL on sites where a high degree of sensitive data transfer occurs or users are apt to use public wireless access points.
- Utilise DNSSEC to further protect a site's DNS infrastructure from attack and exploits.
- Pro-actively scan sites for malicious links, iFrame exploits malware and malvertising.[6]
- Disable SSL 3.0
- Enable TLS 1.2
- Upgrade all SSL certificates to SHA-2, from SAH-2 (Secure Hash Algorithms).

[6] https://otalliance.org/resources/type/advertising-integrity-fraud

SSL IMPLEMENTATION & VULNERABILITY ANALYSIS

Proper and ongoing monitoring of a site's SSL configuration is of critical importance to an organisation's security defense and depth strategy and a first line of defense to minimise external threats. While it is straightforward to obtain and install SSL or EV SSL certificates, care must be taken to maintain a site, with ongoing checks to ensure that the latest protocols and configurations are in use. In October 2014 Qualys Labs found that only 32.8% of the 151,509 sites tested globally were considered secure, scoring 90 points or better.[7]

The overall SSL scores incorporated in the OTA Audit included data from the Qualys SSL Labs, High-Tech Bridge SA and SiteLock as well as data provided by Symantec and Microsoft. Collectively this data was used to evaluate sites' SSL implementation, EV SSL adoption, and vulnerabilities to cross-site scripting, iFrame exploits, malware and malicious links.

In addition to incorporating additional data attributes for the 2014 Audit, testing for HeartBleed vulnerabilities and support of SHA-2 (Secure Hash Algorithm), were included. These enhancements provide a deeper evaluation against current threats.[8] [9] In instances where more than one SSL server or SSL connection was observed, the analysis incorporated the data on the highest scoring server.

As in previous years, OTA's 2014 analysis found cases of mis-configured servers. Where possible, OTA made efforts to contact the server administrators to help them protect their site from the visible exploits by sending email to the contact address at the respective domains. Several sites were able to reconfigure servers to reduce vulnerabilities, and while notification may have resulted in a favorable impact on a site's scores, OTA only utilised the initial score.

Presence of site vulnerabilities including iFrames, XSS and malicious links were observed in less than 3% of all sites. This reflects increased diligence of site owners regarding scanning and securing their server configuration. Sites which accept third-party content and advertising are encouraged to hold their ad partners accountable to security best practices since the levels of malicious advertising (malvertising), has increased in frequency and severity, placing users at risk of key-loggers, ransomware and associated threats.[10]

Site administrators are encouraged to review the SSL Server Rating Guide [11], updated in January 2014, which provides an overview of the assessment methodology and addresses common configuration issues. A useful companion document is the "SSL/TLS Deployment Best Practices" published by Qualys [12]. OTA's experience with these resources and tools has shown that changes can usually be made quickly and inexpensively once technical decision makers are engaged and issues are identified.

[7] Source: Qualys 2014 report https://www.trustworthyinternet.org/ssl-pulse/

[8] https://community.qualys.com/blogs/securitylabs/2014/01/21/ssl-labs-stricter-security-requirements-for-2014

[9] http://heartbleed.com

[10] OTA Advertising & Content Integrity Best Practices https://otalliance.org/resources/advertising-integrity-fraud

[11] https://www.ssllabs.com/downloads/SSL_Server_Rating_Guide_2009e.pdf

[12] https://www.ssllabs.com/downloads/SSL_TLS_Deployment_Best_Practices_1.3.pdf

EXTENDED VALIDATION SSL CERTIFICATES

Extended Validation SSL Certificates (EV SSL) help address lookalike and phishing sites as well as the issue of fraudulently obtained SSL Certificates. EV SSL requires a thorough verification and audit process that helps prevent deceptive and illicit entities from obtaining a certificate on behalf of a legitimate brand. EV SSL provides differentiation and recognition for sites by displaying a green identifier as a visual trust indicator in the address bar or browser chrome.

As illustrated in Figure 7, worldwide adoption of EV SSL certificates continues to increase, growing more than 39% to exceed 103,000 deployed certificates.[13] Growth of SV SSL certificates has been attributed to brands' desire to instill consumer trust of their sites in response to the increased prevalence of phishing and deceptive websites. Further fueling this grow is the baseline requirements of several new gTLDS including .Bank, .Insurance and .Trust requiring EV SSL certificates.[14]

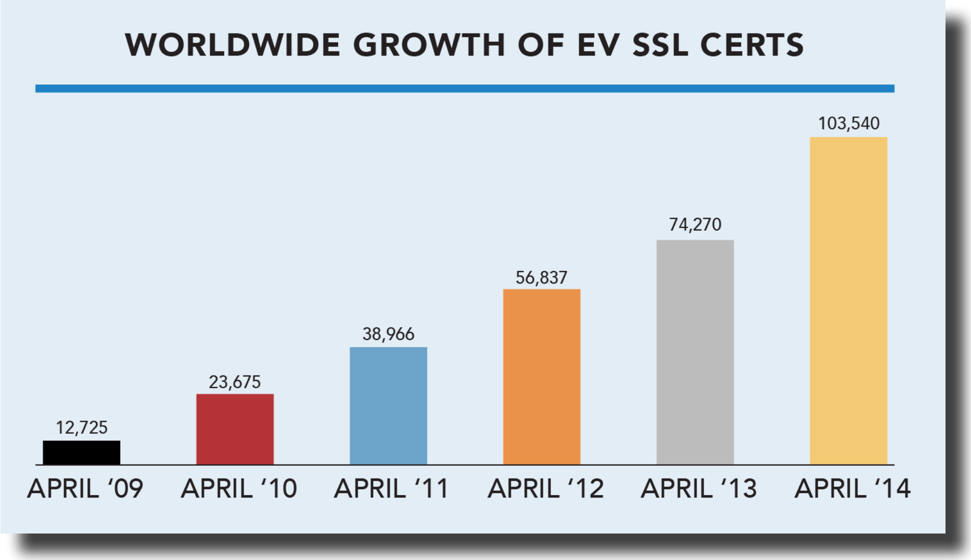

Figure 7 – EVSSL Certificate Growth

DOMAIN NAME SYSTEM SECURITY EXTENSION (DNSSEC)

DNSSEC adds security to the DNS lookup. It is designed to help address "Man-in-the-Middle" (MitM) attacks and cache poisoning by authenticating the origin of DNS data and verifying its integrity while moving through the Internet. DNSSEC is now deployed in the .com, .gov, .org and .net TLD's, and will be supported by several of the soon to be released restricted gTLDs including .Bank and .Trust.

No sites tested have adopted DNSSEC in any of the ANZ 150, consistent with the overall low worldwide adoption. A noted exception is the U.S. Federal 50, with 92% adoption, driven in part by a Presidential directive requiring adoption by U.S. governmental agencies.[15] Broad implementation of DNSSEC has historically been hampered by lack of infrastructure (hosting environments, registrars and browsers) as well as competition from higher priority security projects with an organisation.

[13] Source: Netcraft - www.netcraft.com

[14] http://www.ftld.com/

[15] http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2008/m08-23.pdf

DATA PROTECTION, PRIVACY & TRANSPARENCY

As businesses throughout the world are becoming "data driven"marketers and increasingly collecting data across devices, it is more important than ever for organisations to strike the balance between data collection privacy and data stewardship. OTA has been advocating for increased discoverability and clarity of privacy policies since 2009, recommending policies be written for the consumer (versus an attorney) and provide disclosure of data collection, data usage, sharing and retention practices. The following best practices are generally consistent with the Australian Privacy Principles (APPs), updated in early 2014.[16]

Best Practices:

- Publish discoverable, easy to find, and comprehensible privacy policies.
- Create a layered, concise summary linking to an expanded policy. Provide a clear detailed statement regarding whether personal data is being shared with third parties, what data is being shared and why it is being collected. See OTA short form, linking to the full policy - http://otalliance.org/privacy-policy.
- Write policies for the site's target audience and demographics. Consider providing bi-lingual versions representing the diversity of non-English speaking site visitors. As an example see Spanish version of OTA's privacy policy – https://otalliance.org/politica-de-privacida.
- Share details of data retention policies including clarification on the duration such data is retained after the online account is terminated.
- Make best efforts to provide notice to consumers if their data is requested by third parties due to legal requirements. Suggested draft copy includes the following statement "To the extent we are legally permitted to do so, we will take reasonable steps to notify you in the event that we are required to provide your personal information to third parties as part of legal process." [17]
- Utilise tag management systems or privacy solutions to help manage third-party trackers and to help ensure they are acting properly.
- Disclose whether the site honours Do Not Track (DNT) settings in the site's privacy policy, and preferably respects users' DNT browser settings. While such disclosure is now required for sites with users who reside in California, due to the recent passage of the regulation, this requirement was classified as bonus points for this year's Honour Roll.

As outlined in the Methodology, several criteria were added as bonus opportunities this year, including the use of layered privacy policies, disclosure of a site's DNT policy, and use of tag management or privacy solutions. These emerging best practices add to the analysis of privacy policies, site tracking, public vs. private WHOIS registrations, honouring of DNT and data loss incidents. By looking comprehensively across these criteria, it is possible to get a complete view of a company's commitment to privacy and their respective business practices.

[16] http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles

[17] Sites should conduct a legal review to ensure this draft copy is applicable to their business models and regulatory requirements.

PRIVACY POLICIES & PRACTICES

Privacy scores were determined through a combination of evaluating a site's privacy policy including disclosures, policies and design, disclosure of honouring Do Not Track (DNT), use of tag-management / privacy solutions and past data breach incidents. Sites were scored on a scale of 100 points, with 50 points possible for evaluation of the site's privacy policy, and 50 points possible based on the privacy qualifications of third-party trackers seen on the site.

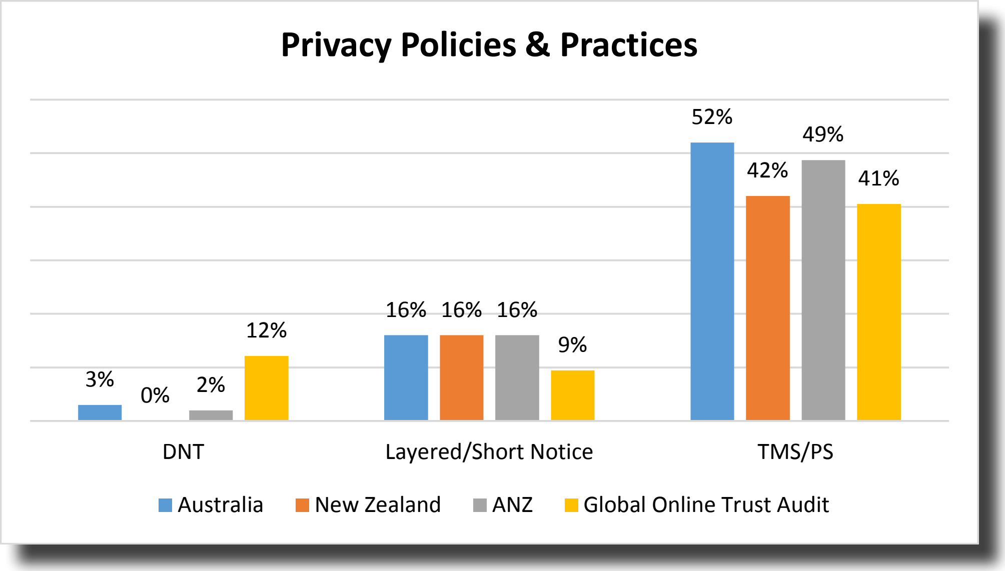

Figure 8 – Privacy Practices

The ANZ outscored other geographies in the adoption of layered notices which has been driven in part by the practices of linking to standard government privacy policies and may be overstating the metric of providing users short concise notices. As DNT becomes a legal requirement in many geographies, OTA believes it will become increasingly important for sites to both disclose their DNT policy as part of their privacy policy and to honour the user's browser DNT setting. It is important to recognise this requirement is not based on where a company may have a nexus or physically operates, but where the user resides. As sites frequently do not know where their users reside it could have significant impact. In North American this requirement has been driven by the State of California. As of the date of this report other states, provinces and the European Union have not passed such requirements.

Sites which rely on advertising and third-party analytics are faced with a complex and dynamic challenge of managing third-party tracking, which can create conflict with the stated privacy policy and regulatory compliance. Tag management and privacy solutions are becoming a best practice to allow review and monitoring of data collection and sharing in real time. ANZ again outscored the Global Audit by nearly 20%, or 8 percentage points. OTA utilised site scanning capabilities to detect such systems and awarded bonus points if they were present.[18]

As witnessed, no organisation is immune to data breaches and often such incidents can be indicative of inadequate security practices, potentially impacting a site's brand reputation and trustworthiness. Unlike the data published in North America and other regions, public data on breaches and related data loss incidents in Australia and New Zealand was very limited, and may have provided a positive bias to the ANZ 150 as no sites received negative scores related to data breaches.[19]

[18] Site scanning provided by InfoTrust http://infotrustllc.com and Ensighten

[19] This may change if the Privacy Amendment (Privacy Alerts) Bill 2014 is passed, which would require mandatory notification http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s958

CONCLUSION

The security and privacy landscape continues to evolve as new and innovative data driven services are being introduced while data breaches and privacy missteps are becoming common occurrences. In general the ANZ 150 is lagging behind the Global Honour Roll, in part due to their relatively smaller size and an apparent lack of general awareness of some of the emerging standards and best practices. As pending privacy and data security legislation moves forward, the awareness of such measures is expected to influence the adoption of the best practices prescribed in this report.

The initial ANZ Online Trust Audit revealed several significant variances, primarily in email protection and privacy enhancing best practices, while server security is on par with other geographies. This report reveals several simple to implement best practices to help enhance consumer and brand protection from spoofed and malicious email. Concurrently, sites are encouraged to increase the disclosure of their data collection, data usage, retention and sharing practices. While one's existing policies may being in compliance with current regulatory requirements, to maximise consumer trust sites are encouraged to increase transparency of their practices and move to a view of stewardship, looking at the long-term interests and needs of their site visitors and customers.

Highly publicised failures and vulnerabilities have a negative impact on consumer trust. Left unchecked and without a commitment to meaningful self-regulation and enforceable codes of conduct, the reputation of brands and the health of the Internet itself are at risk. As the world economy, society and critical infrastructure become increasingly reliant on the Internet, it is incumbent on the business community, associated trade organisations and governments to embrace these practices moving from a compliance mindset to one of stewardship.

The OTA Online Trust Audit and Honour Roll highlights proven best practices and recognises those companies which have demonstrated a commitment to consumer safety, security and privacy. Companies that earned Honour Roll status are to be commended and serve as a "North Star" for others to aspire to.

Adoption of the outlined best practices serve as the foundation of meaningful self-regulation. Companies who adopt these and other security controls should be afforded protection from onerous regulatory oversight and receive "safe harbor" from frivolous lawsuits. The 2014 Audit confirms a renewed commitment to stewardship and adoption of best practices. This report serves four primary objectives:

- Recognise leadership and commitment to best practices which aid in the protection of online trust and confidence in online services.
- Promote best practices and provide tools and resources to aid companies to enhance their security, data protection and privacy practices.
- Raise awareness of risks, helping businesses to improve their security and privacy practices.
- Aid consumers in making informed decisions about the security and privacy practices of sites they frequent.

To maximise consumer protection, no single company or constituency can work alone. Only with the collaboration of industry, business, NGOs and government stakeholders can we achieve a "trusted Internet" and assure the vitality of online services.

ACKNOWLEDGMENTS

Data and analysis has been provided in part by: Agari, AVG Technologies, Bounce.IO, comScore, DigiCert, Ensighten, GlobalSign, High-Tech Bridge SA, IID, InfoTrust, Microsoft, Qualys, Return Path, SiteLock, SSL Labs, Symantec and TRUSTe. Special thanks to Jeff Wilbur OTA Board member, OTA strategic advisors Mary Berk, Barry Brailey and Mark Goldstein and Arun Raghu for their review and insights.

Updates to the report including the 2014 Global Honour Roll Audit and report may be found at https://otalliance.org/HonourRoll. To submit comments or suggestions, email editor @ otalliance.org.

ABOUT ONLINE TRUST ALLIANCE (OTA)

The Online Trust Alliance (OTA) is a non-profit with the mission to enhance online trust and user empowerment while promoting innovation and the vitality of the Internet. Its goal is to help educate businesses, policy makers and stakeholders while developing and advancing best practices and tools to enhance the protection of users' security, privacy and identity.

OTA supports collaborative public-private partnerships, benchmark reporting, and meaningful self-regulation and data stewardship. Its members and supporters include leaders spanning public policy, technology, e-commerce, social networking, mobile, email and interactive marketing, financial, service provider, government agency and industry organization sectors.

OTA is a 501(c)3 tax exempt global non-profit focused on enhancing online trust with a view of the entire ecosystem. OTA is supported by donations and support across multiple industries, representing the private and public sectors. To support OTA visit https://otalliance.org/donate.

Material in this publication is for educational and informational purposes only. Neither the publisher, the Online Trust Alliance (OTA), its members nor the authors assume any liability for any errors or omissions nor how this publication or its contents are used or interpreted or for any consequences resulting directly or indirectly from the use of this publication. OTA makes no assertions or endorsements regarding the security, privacy or business practices of companies that may choose to adopt such recommendations outlined. For legal advice or any other, please consult your personal attorney or appropriate professional. The views expressed in this publication do not necessarily reflect the views of OTA member companies or affiliated organizations.

OTA MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. No part of this publication may be reproduced or distributed in any form or by any means, or stored in a database, web site or retrieval without the written consent of OTA.