Sentria

Cybersecurity:
The State of Australian Websites

April 2022

About Us

Sentria is a new Queensland-based provider of website security services, partnered with CyberTzar, a UK-based SaaS (software as a service) platform provider offering cyber risk assessment and management with a focus on websites and servers.

Created by a team of leading technologists responsible for delivering a substantial number of £ multi-million critical IT infrastructure projects for the UK Government and others, Directors include a former (UK) CTO of Sun Microsystems, senior computer scientists within academia as well as infrastructure heads within major blue chips, banking and the public sector, including the police.

Built initially for their own use in the absence of any existing technology deemed suitable, a decision was taken in early 2021 to make the solution publicly available at the end of Q4 of that year with first website data collated in Qs3 & 4. Shortly afterwards CyberTzar announced a strategic partnership with the West Midlands Cyber Resilience Centre (WMCRC), a (UK) Home Office-initiated not-for-profit partnership between policing, academia, private industry and third and public sector organisations working to support and protect businesses in the region and UK as a whole against cyber threats.

Sentria is the exclusive partner of Cyber Tzar in Australia, and provides businesses with website remediation and security management services. Research into the (cybersecurity) state of Australian websites commenced in Q3 2021 and forms the basis of this Report.

Executive Summary

Australia has an acknowledged cybersecurity problem which last year cost the economy some $33 billion[1][2]. Additionally, research shows 50% of all data breaches begin with web applications[3] while Australia and the APAC region saw a 38% increase in such attacks on the financial services sector between January and June of last year alone[4].

Using the CyberTzar platform[5] - a UK-based SaaS business which assesses and manages cyber risk of websites, web applications and servers - we set out to explore the security and integrity of Australian websites by conducting technical scanning of hundreds of high-profile sites (around 1,000 currently) across a variety of business sectors, undertaking static code tests to check every known vulnerability in all visible areas of sites tested.

The platform conducts over 55,000 checks by automating the OWSAP Zap open-source web application security scanner[6] then generates a standardised 'cybersecurity score' (out of a possible 1,000) providing a clear indication of the risk impact and risk distribution of technical vulnerabilities found in a given website – for this report scanning was limited to website static code only, equivalent to search engine website scanning.

Sites surveyed were intended to be as representative as possible of the Australian web landscape generally and were selected by taking a relatively small but meaningful sample from a number of business sectors reflecting the fact that sites can vary in function and purpose.

Content Management Systems were also checked to establish 'baseline scores' from which it becomes possible to determine an upward or downward trajectory in a site's security as a result of back-end or front-end development work.

Sectors examined were as follows, with descending cybersecurity scores averaged within groups:

- e-Retailers (Average 680)
- jobactive Providers (Average 553)
- Food Manufacturers (Average 549)
- Top 100 Accountants (AFR List 2020) (Average 535)
- Businesses Local to this Report's Authors (Average 533)
- Charities (Average 522)

The average score in aggregate was 562.

To provide context to this, were scores to be placed on a sliding scale of 0-1000, as a rule of thumb one could say:

- 1 – 400 requires immediate attention. Very attractive to the potential cyber-criminal;
- 400 - 700 requires immediate attention;
- 700 - 900 near term action recommended;
- 900 - 1000 low priority action required.

Websites of Australia's 'Top 100 Web Development Agencies' (according to The Manifest 2020 list)[7] were also checked, since such organisations undertake the majority of the country's back- and front-end creation, and had an average score of 560.

Further technical & data analysis of test results also revealed that while '**High Impact' vulnerabilities accounted for only around 20% of all those discovered, over 95% of sites scanned contained one or more of these vulnerabilities within their static code.** Full penetration testing would be highly likely to reveal more still.

Scores themselves – pointing to mediocrity of security rather than excellence or inferiority generally speaking – showed some differences between business sectors, with especially serious issues found in a number of sites individually and within certain sectors in particular, for e.g.:

- **e-Retailers scored** higher on average than other sectors but up to 50% of the sites checked could be open to data breaches. These include extremely high-profile companies/brands.
- **100 Top Web Development Agency** results suggested, in many cases, that cybersecurity is not a priority; a quarter of sites scored poorly. While a correlation seemed to exist between poorly scoring agency sites and the sites of those agencies' clients, *no* real correlation was found between agencies whose sites scored well for cybersecurity and the security of those of their clients - suggesting a disconnect between ongoing maintenance provision after project completion.
- **jobactive Providers** are subject to the Federal Government's new Right Fit for Risk regulations[8] and moreover are quasi- Governmental organisations, a higher standard of website security was anticipated but not found. Inadequate site maintenance appeared responsible for the majority of vulnerabilities discovered.
- **Food Manufacturers** - though not decisively better or worse than any other sector surveyed - contained at least one instance and probably more of an entire supply chain being at high risk of a successful cyber-attack.
- Around a third of the **Top 100 Accountants** scored particularly poorly, including some larger firms. While many of the sites functioned mainly as 'brochureware', a significant number offered client log-in privileges including at least one with an extremely vulnerable site overall. Moreover, webforms commonly used (as in all other sectors) for e.g. email contact were often found to be vulnerable to Cross Site Scripting attacks[9], risking servers and sites as a whole.
- Where '**Local Businesses**' (to this Report's authors) were concerned, one web agency dominated the market – and with a poor-scoring site itself, had built a large number of other sites themselves scoring poorly. Business owners seemed indifferent to cyber threats despite (in one case) having been subject to more than one attack.
- **Charities'** websites were particularly disturbing collectively speaking since many accepted and encouraged online donations, including sites that were especially vulnerable and belonging to very well-known organisations.

Conclusions

Results strongly suggest a pervasive problem with security among many - probably most - Australian websites, which generally speaking are vulnerable. Given this, it is not surprising that cybercrime, particularly directed toward websites and web applications, continues to rise.

Most websites surveyed were at risk, or high risk, of various types of serious cyber-attack, some with potentially dangerous consequences both for site users and the organisations concerned.

The authors therefore conclude action on cybersecurity has not risen to an appropriate level of importance/ significance in business and IT management, which requires both ongoing website maintenance and regular testing of vulnerabilities to be broadly adopted.

Introduction

Much is written and spoken about daily in Australia in respect of the continued and growing threat of cybercrime - not least by a Federal Government clearly frustrated at the response by many in the business community[10].

From annual data shared annually by the Signals Directorate's Cyber Security Centre (ACSC) - established to coordinate and assist with Australia's response to increased cyber-attacks globally - it's easy to see why.

Australia is the sixth most cyber-attacked country in the world according to the WEF Global Risks Report 2021[11] and over half of Australian businesses have been subject to such attacks The Australian Financial Review has reported[12] .

These statistics are borne out by the ACSC itself which says there were over 67,500 cyber-attacks reported in Australia over the last financial year, an increase of nearly 13% from the year previous. Many though go *un*reported[13].

Of those that *are* recorded however, small businesses made a higher number of cybercrime reports than in previous years and medium businesses had the highest average financial loss per report, costing them respectively on average $8,899 (for the former) & $33,442 (for their medium-sized counterparts)[14].

Over 1,500 known incidents of malicious cyber activity were related to the coronavirus pandemic (approximately 4 per day) and there were over 500 ransomware cybercrime reports in 2021, an increase of nearly 15% from the previous year[15][16].

Meanwhile, AUSTCyber – a further Government initiative created to encourage and help develop increased sovereign cybersecurity capability in Australia - found in a survey undertaken as part of its 2020 Sector Competitiveness Plan[17] that various important industry sectors (healthcare and social assistance, research, education & training, manufacturing, transport & logistics along with wholesale and retail trade) were at 'high' or 'very high' risk of being subject to a 'cybersecurity shortfall'[18].

While the research and reporting by the ACSC, AustCyber and others provide indispensable insight into an ever more serious and widespread issue, our own Report (the first of what is envisaged as a regular series) deals with just one aspect of the cyber threat landscape – the security of Australian websites.

Though the research being presented below is unique – to our knowledge no other organisation has conducted and then collated the results from technical tests of hundreds of sites (over 1,000 currently) across a variety of business sectors – nevertheless some further, more specific context is helpful.

This comes in the shape of a 2021 study by the labs of cybersecurity giant Imperva of around 4.7 million web application attacks globally[19]. It found not only are such incidents increasing on average by 22% per quarter, no fewer than **50% of all data breaches begin with web applications**. A 67.9% jump in attacks was seen between Q2 & Q3 of last year and in Britain attacks have increased by 251% since October 2019. Australia and the APAC region meanwhile have seen a 38% increase in web app attacks on the financial services sector alone between January and June 2021.[20][21][22].

To the above it needs to be added that an ever-increasing number of cyber-attacks are carried out automatically by 'bots' crawling the web seeking out and exploiting vulnerabilities with little or no human intervention, making certain types of website attack a near inevitability.

Meanwhile, attacks are expected to grow in frequency, potentially rapidly, as malicious software availability increases.

According to another Report from Imperva – the 'Bad Bot Survey 2021'[23] automated malicious software represents a 'pandemic of the internet' with 'bad bots' now accounting for 25.6% of all Internet website traffic.

Of these, says Imperva in the above Survey:

> *'Advanced persistent bots (APBs) remain the majority of bad bot traffic, amounting to 57.1%. These are a combination of moderate and sophisticated bad bots that are harder to detect and mitigate. They cycle through random IPs, enter through anonymous proxies, change their identities and mimic human behaviour'.*

It is in light of all this that our own research was conducted.

If Imperva and the ACSC provide many of the '*whats and wheres*' of cybercrime generally and web application attacks in particular, our own efforts seek to go some distance in asking (and demonstrating some answers to) the questions of '*how and why*'.

Scoring

The CyberTzar score provides an indicative number out of 1,000 of the risk of websites, web applications and servers falling victim to a cyber-attack.

Automating the OWASP Zap[24] open-source web application security scanner, the CyberTzar platform scans websites, web applications and other online assets for all known security vulnerabilities, ranging from 'built in' problems such as weaknesses in configuration or errors in coding to 'maintenance' problems such as out-of-date security protocols or coding libraries as well as 'new' (previously unknown) exploits.

Score calculations are undertaken by an algorithm using the latest (2021) OWASP Top 10 guidance[25] for the most critical web application security risks representing consensus among security experts from around the world based on the frequency of discovered security defects and severity of the vulnerabilities.

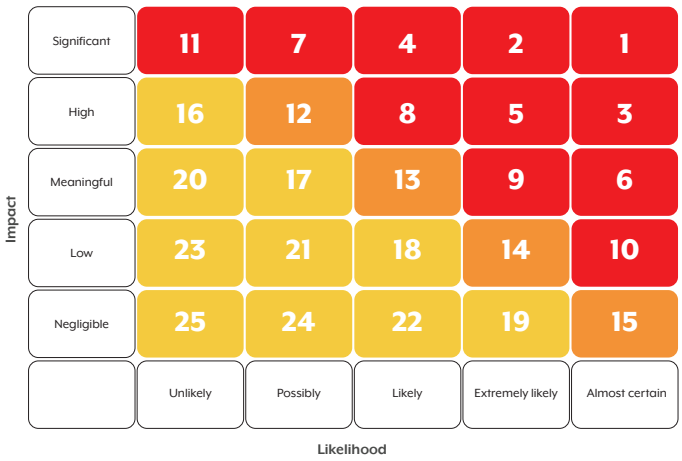


Fig. 1 Standard Risk Matrix with Risk Groups

CyberTzar's own team has furthermore cross-mapped the OWASP Top 10 against relevant elements from the NIST 800- 53[26] & MITRE ATT@CK[27] Frameworks, keeping such vulnerabilities under constant review and assigning each to one of 25 risk categories as shown on a standard Risk Rating Matrix[28].

Using this matrix, the 25 'Security Groups' are each then further assigned to the three 'Risk Groups' of 'Red' (suggesting areas of priority for immediate action) 'Orange' (suggesting areas of priority for near-term action) and 'Yellow' (suggesting slightly lower priority areas for longer-term action – see Fig. 1 left).

Put another way, risk can be considered as follows:

1. Super low (groups 23 - 25)
2. Low (groups 16 - 22)
3. Edge/Border (groups 12 - 15)
4. High (groups 4 - 11)
5. Super High (groups 1 - 3)

Scores are thus derived from individual vulnerabilities identified, weighted by the security group to which they have been allocated.

Based on these same allocations, CyberTzar also generates Risk Impact Distribution and Risk Impact Assessment Matrices shown in Figs. 2 & 3 (below), the latter of which places vulnerabilities within individual risk groups depending on the potential impact of a cybersecurity breach and the likelihood of an attack taking place.

'***Impacts***' are rated from 'Negligible' to 'Almost Certain' and are defined as follows:

'Negligible' – A vulnerability with a negligible impact is one which is not on its own a major a major concern but which might enable or facilitate other attacks;

'Low' – A vulnerability with a low impact is one which, if exploited, might impact a single user session and include compromising user data and, potentially, payment information;

'Meaningful' – A vulnerability with a meaningful impact is one which, if exploited, might impact multiple user sessions again compromising user data and, potentially, payment information;

'High' – A vulnerability with a high impact is one which, if exploited, might facilitate access to, and theft of, large amounts of user data whilst the site continues to operate;

'Significant' – A vulnerability with a significant impact is one which, if exploited, might lead to a massive loss of user data, payments information and bring the site down altogether, causing the business to cease operating online if no back-up exists.

'*Likelihood*' is rated from 'Unlikely' to 'Almost Certain' with categories defined as follows:

'Unlikely' – The exploitation of a vulnerability is deemed to be 'unlikely' if there are no, or very few, known attacks based on the vulnerability or if knowledge of the exploits that do exist is very rare;

'Possible' – The exploitation of a vulnerability is deemed to be 'possible' if there are known exploits that knowledge of such exploits is uncommon;

'Likely' – The exploitation of a vulnerability is deemed to be 'likely' if there are known exploits and knowledge of such exploits is widely distributed;

'Extremely Likely' - The exploitation of a vulnerability is deemed to be 'extremely likely' if there are known exploits with knowledge of such exploits widely distributed and tools (programs) have been developed to automatically seek out and exploit these vulnerabilities;

'Almost Certain' - The exploitation of a vulnerability is deemed to be 'almost certain' when there is very widespread adoption of easy-to-use automated tools used to 'spider' across the web seeking to exploit a given vulnerability in every online asset they can find. In this case we argue it is only a matter of time before an exploit is effected.

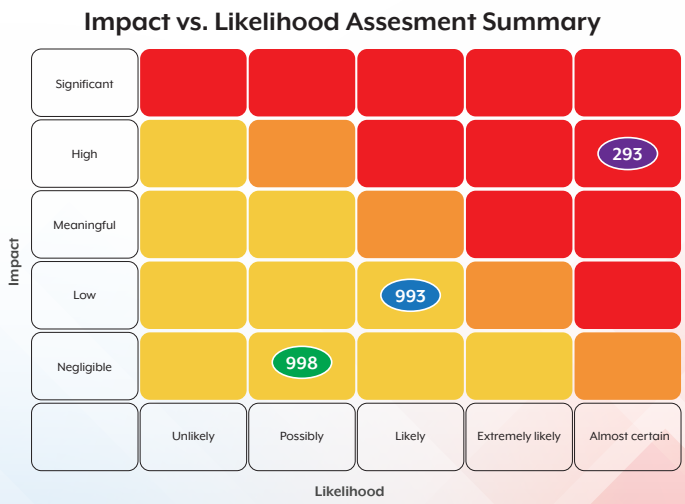


Fig 2. Typical Risk Impact Assessment Matrix

The Risk Impact Assessment ("RIA") summarises your current score position, **293** (Purple Oval), in highest risk group discovered.

A suggested priority for remediation based upon severity is below. The resultant score would be **993** (Blue Oval).

- Vulnerable JS Library (type:72)
- Vulnerable JS Library (type:35)
- Vulnerable JS Library (type:64)
- Sub Resource Integrity Attribute Missing
- Source Code Disclosure - PHP
- Source Code Disclosure - SQL
- Dangerous JS Functions
- Server Leaks Version Information via "Server" HTTP Response Header Field
- Strict-Transport-Security Header Not Set
- Content Security Policy (CSP) Header Not Set (type:2)

Addressing all but the least severe vulnerability results in a score of **998** (Green Oval); address 3 additional items.

Use the online "re-score" function to exclude individual risks to understand the impact of remediation efforts.

Key

Immediate Action	Current score position
Near Term Action	Post immediate & near-term action
Low Priority Action	Best possible score position

CyberTzar's Risk Impact Distribution Matrix (Fig. 3) uses the same axes and definitions as above, this time indicating the distribution of vulnerabilities across the website and their severity. The size of the oval in each section reflects the contribution of the vulnerability to the overall score, influenced by the number of different types of vulnerability to that risk group categorisation.

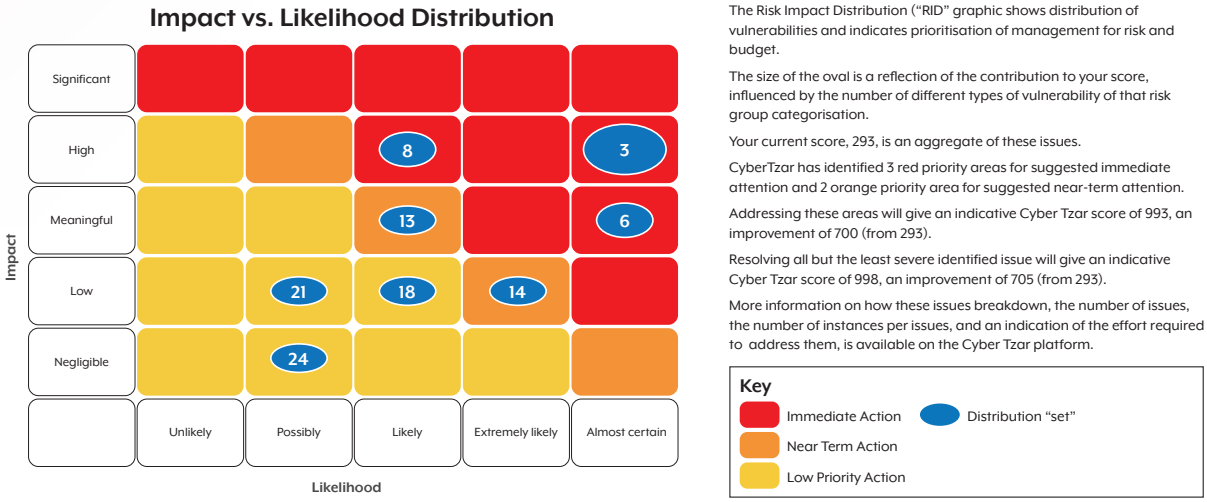
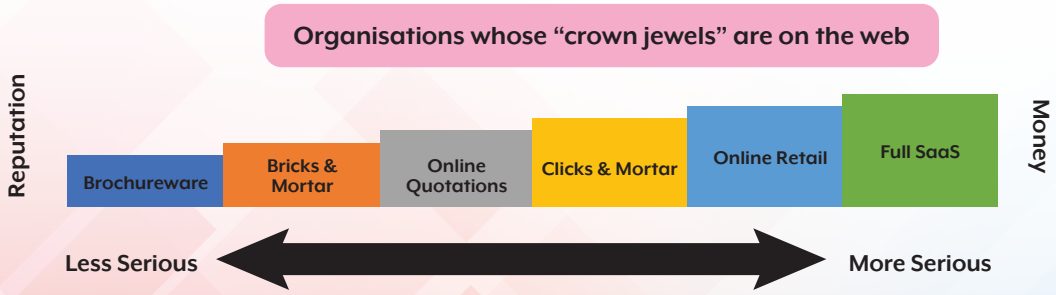


Fig 3. Typical Risk Distribution Matrix

While the relative merits or otherwise of the weightings and risk/security groups attached to each vulnerability or category of vulnerability may be debated by professionals within the IT security industry, the discussion is largely an academic one. What is *not* up for debate is that such vulnerabilities (whatever the seriousness of their risk profile) exist in the websites examined for this Report, and are exploitable – with many prone to opportunistic attacks by 'bots' 'crawling' the internet in search of them. Indeed, as already indicated, it is the growing prevalence of this non-human activity that leads the developers of the CyberTzar platform to categorise the likelihood of some of these exploits as 'Almost Certain'.

With that said however, scores are based purely on the *technical risk* of a cyber-attack – *business risk* (the effect such an incident would have on an organisation) would clearly require specific understanding of, for example, that organisation's regulatory compliance requirements, loss of revenue for website downtime, the reputational damage of a data breach or any other factor relevant to assessing the effect on a business of a successful website or web application attack.

In short, only a business owner and/or experienced actuary can calculate damage to the business such attacks might incur, likely determined by the function and importance of a website/online presence as suggested in the below graphic.



Methodology

It's not possible to know exactly how many websites exist in Australia but there are just under 3.5 million .au domains registered and administered by auDA[29], the organisation responsible for governing the .au country code Top Level Domain - and in all probability most registrations represent some kind of web presence. To these can be added Australian businesses that use non- .au domains (such as .com) – an unknown but considerable number.

CyberTzar itself holds a database of over 9.5 million companies and accompanying website domains worldwide, around 263,000 of which are companies with .au domains headquartered in Australia. Though a future phase of development will see testing and monitoring every one of the sites in this database - thus creating unrivalled knowledge of the security profile of websites globally - in these early stages, and for the purposes of this Report, our objectives were rather more modest.

The aim was to create a snapshot of how vulnerable – or resilient – a small but meaningful sample of Australian websites may be to cyber-attack, and based on this draw attention to issues raised in the hope that website and web application security is prioritised in the creation and maintenance of sites moving forward.

Thus, using the CyberTzar platform we carried out full-site static code tests of around 1,000 selected, often high-profile websites domestically.

Site Selection

The below model elaborates on the smaller-sized version on the preceding page, broadly depicting most types of website, its function within an organisation and the possible or likely severity of a successful web application cyber-attack on a business. It should be noted however that, even if a site is completely static and non-transactional, meaning no direct financial loss or significant data breach could possibly result from an attack, reputational damage of a hacked site to a business might be considerable. As one CEO put it during an interview: '*We don't want to end up on the front page of the paper because our URL was redirecting visitors to a porn site.*'

Thus, while there is no doubt a successful cyber-attack would prove disastrous for some kinds of organisation (those tending rightward on the graphic) for those tending leftward, consequences may be of greater or lesser importance.

Taking the above into account, we therefore selected sites we felt were generally reflective of all but one of the above categories ('Full SaaS') since these businesses and the services they offer should (one would hope) already be subject to the highest standards of cyber security available.

The public sector was deliberately omitted altogether since this is deserving of its own, separate survey.

To reflect the remaining columns therefore we selected an initial four business sectors these being:

1. Food Manufacturers
2. E-Retailers
3. Charities/Not-for-Profits
4. Accountants

Further rationale behind choosing these sectors was that some (food manufacturing, retail) have been identified as being at 'high' or 'very high' risk of being subject to a 'cybersecurity shortfall'[30] while others (charities, accountants) were likely to at risk of reputational damage and/or subject to strict regulatory/compliancy issues.

Various other miscellaneous sites were also examined for a variety of reasons, discussed below.

Selection was made using lists of companies or websites found on the internet, e.g.:

- The 2020 AFR list of Top 100 Accountancy Firms[31]
- Sites associated with the 2020 Inside Retail 'Top 50 People in e-Commerce' awards plus other online lists such as the Store Leads App[32] [33]
- Selected charities from the Australian Charity Guide[34]
- The Top 100 Food Manufacturers listed by Food & Drink Business Magazine[35]

Further Sectors: Right Fit For Risk – ISO 27001 Certification

As well, the Australian Government, via the Department of Education, Skills and Employment, has mandated that all providers of skills/employment training and disability employment services need to become ISO 27001[36] compliant under a scheme called 'Right Fit For Risk'[37]. ISO 27001 is a global information security framework/standard. For this reason, we additionally scanned websites of the 40 current jobactive Providers in Australia (many of which also provide further services which would be subject to the scheme) since we felt such an exercise may or may not be indicative of information security standards more generally within that sector.

Web Development Agencies

As *architects and creators* of many of the websites concerned, web development agencies clearly play a major role in the security of the sites they construct, hence we additionally tested sites belonging to the 2020 list of 'Top 100 Australian Web Development Agencies' according to The Manifest[38] (part of the clutch.co group) to check, *prima facie* the priority given to cybersecurity by website professionals.

We further tested a variety of these agencies' client sites where a given agency was known to have been responsible for a particular website. Identification of these clients was undertaken by examining the public portfolios of top and bottom performing deciles of the 'Top 100' agency websites and a randomly selected number 'in between'.

Most testing was carried out in late August 2021 with some follow-up (re)testing of selected sites carried out between November 2021 – February 2022.

Content Management Systems (CMS) and e-Commerce Platforms

Given the propensity for web development agencies to use popular CMS and e-Commerce platforms we tested and scored a group of what are essentially the 'main providers' of such solutions scanning straight 'out-of-the-box' vanilla installs to understand site security without intervention. Using these baselines, it thus becomes possible to assert that any upward or downward deviation is as a result of development work on these platforms.

While not completely exhaustive, the below (which were those tested) represent the main platforms employed accounting for the vast majority of websites.

- Wordpress
- Wix
- Squarespace
- Shopify
- Magento
- Joomla
- Drupal
- BigCommerce

Miscellaneous Sites Tested

In addition to sites belonging to clients of various of the 'Top 100 Web Development Agencies', some testing was also carried out on a local (geographical) basis in Central Queensland, where Sentria as a company is based.

A modest selection of prominent business websites were examined along with local web development agency sites, the latter accompanied by an additional number of client sites within and outside of the area. Agencies responsible for the websites of the 'prominent businesses', which included those in the financial and legal sectors, were also tested.

Further Qualitative Data

A number of interviews - either by telephone or email - were carried out with selected site owners or managers from all categories mentioned above although it became quickly clear that an entire (and sizeable) piece of further research will be necessary to establish a more cogent appraisal of attitudes toward cybersecurity in general and web/web application security in particular. Any information derived from this source is therefore illustrative only.

In the meantime, PWC undertakes an annual 'CEO Survey'[39] which – as in previous years – emphasised respondents' concerns over cybersecurity[40] thus making possible a comparison between what key individuals say publicly about the matter and the actual state of affairs.

In conclusion, while the total number of sites tested accounts for only a drop in the ocean in terms of the overall volume, the selection criteria provide for a fair reflection of a reasonable variety of websites found in Australia.

On that basis we feel this initial Report offers both an accurate snapshot and sufficiently valid assessment where their cybersecurity is concerned.

Results

General Points

While we believe them to be of considerable value and interest, the following results do however need to be prefaced with a number of significant caveats.

Firstly, it's important to note the website and web application security landscape is ever-changing and highly dynamic in nature, particularly where frequent site updates/additions or alterations occur often. With novel vulnerabilities or automated attacks regularly being discovered together with the ongoing release of new coding libraries, a high cybersecurity score one day might drop considerably a week or even a day later (if - for e.g. - a new JavaScript library is released and the site isn't updated). The scores shown here therefore represent only a depiction of what things were like when testing was undertaken (mostly around August/September 2021). Since that time individual scores may have deteriorated – or improved – markedly.

To ameliorate this possibility, we re-tested a number of sites (roughly 15%) that had achieved either particularly high or low scores following the initial scan or because we were in dialogue with owners or managers for the purposes of composing this Report. With only a small number of exceptions (for example, an accountancy firm's site fell by ~ 35% over a four-month period while one jobactive Provider's site *rose* by a similar %age in six weeks) the majority of sites re-scored remained within a 0.5% deviation upward or downward of their original score.

Therefore, while this Report depicts a snapshot of security as they were at the time tests were done (August 2021 onwards), little evidence exists to suggest a dramatically different overall scenario would in any likelihood exist six to eight months later (March 2022).

Secondly, the tests carried out are themselves somewhat limited in scope. Static code (or 'surface' or 'passive') testing - also known as source code analysis - looks for issues within a website's visible code. As such, while thorough, this exercise does *not* seek to exploit vulnerabilities in the way a full penetration test would. Put bluntly, a static code test *can* identify why and where a site is particularly vulnerable, but is *unable* to determine its overall security. Sites with a high score therefore may not necessarily be completely secure (a full penetration test would be required to ascertain this) whereas a low-scoring site most definitely *is not* secure.

Thus – and crucially - full penetration testing, including of all static code, would without question reveal a significant number of further vulnerabilities static code testing alone would not discover.

With this in mind, the below results do however strongly indicate a *pervasive cybersecurity problem among many Australian websites.*

Exceptions to this do of course exist and can often be found among those created, hosted and maintained by long-established and sizeable digital marketing services/review or online stores operated by well-resourced and highly expert digital delivery teams. Though such results are what one might expect from among the major high street retailers and high-profile e-commerce concerns, not all such organisations performed outstandingly well.

As discussed in the preceding section, testing took place among various main 'types' of business, each of which, when averaged, showed a similar score range (of between 533 – 560) apart from e-Retailers which on average (and perhaps reassuringly) scored significantly higher.

AVERAGE SCORES PER BUSINESS TYPE

Group	Average Score
e-Retailers	680
100 Top Web Dev Agencies	560
jobactive Providers	553
Food Manufacturers	549
Top 100 Accountants	535
'Local Business'	533
Charities	522
Aggregate Average	**562**

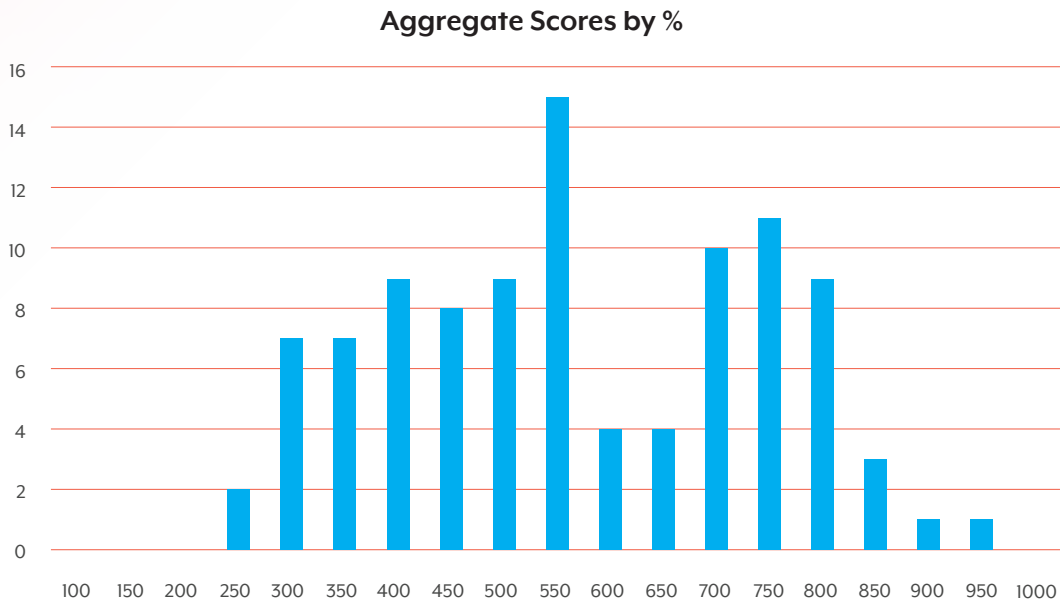
While each business group and its scoring are briefly discussed separately, aggregate scores have also been expressed graphically on the following page, giving an indication (by %) of distribution across all sites tested and discussed in this Report

Notwithstanding a dip in frequency of scores within the 600-650 range (noticed across all sectors except 'jobactive Providers' and probably due to use of CMS, plug-ins and customization patterns), the graph nevertheless does show a significant bell curve from the very poorly scoring sites to those scoring more highly. The clear preponderance of 'middle- ranking' scores is thus generally suggestive of mediocrity rather than overall inferiority or excellence where the security of Australian websites is concerned.

For additional context to this scoring, our technical team were asked to place ranges on a 'sliding scale' from 1-1,000 indicating a site's security status which was as follows:

- 1 – 400 requires immediate attention. Very attractive to the potential cyber-criminal. Development of a remediation plan action, and re-scan urgently needed;
- 400 - 700 requires immediate attention. Development of a remediation plan, action, and re-scan highly recommended;
- 700 - 900 near term action recommended. Actively monitor and improve site security using remediation guidance from e.g. the CyberTzar platform or other;
- 900 - 1000 low priority action required. Continuous improvement plan and regular scans recommended to ensure existing issues and vulnerabilities are not reclassified (due to automation of cyber-criminal tools). Near term action: actively improve site security using the remediation guidance from e.g. the CyberTzar platform.

Aggregate scores in graph form follow on next page.



On a final note, since the CyberTzar platform generates hundreds of pages of data per scan usually unearthing vulnerability issues of varying severity (the majority being fairly minor) that can amount to thousands in number, scope of this Report has been limited to 'top level' results only.

A more detailed Technical Report relying on multiple data points to provide adequate power will follow later in the year. This will explore possible relationships between software use, customisation/development of varying types alongside any links found between these and the frequency of vulnerabilities discovered.

For immediate purposes however, and to in order to offer at least some basic technical insight and inferences, ten websites from five of the selected business groups were used as exemplars of high-, low- and mid-scoring participants in the overall survey and then manually checked by our team.

Where suppositions from these manual findings were felt to be sufficiently robust, they were further checked against a random sample of the general survey population to corroborate or contradict their validity.

Such exercises aside however, we can nevertheless assert with high confidence the below graphs relating to each business sector are reasonably reflective of the security status of websites within respective groups.

Other findings – inferred from the sampling exercise referred to above – are probably best noted in advance since they provide useful accompanying insight to the overall results - though will be likely unsurprising to those armed with any technical knowledge.

For example, around 80% of sites tested used a Content Management System (CMS) with only around 5% using an ERP (Enterprise Resource Planning) solution such as Salesforce, SAP or other such large applications[41]. Around 15% used a custom solution built on PHP frameworks such as Laravel, CodeIgniter or Firebase[42] rather than a CMS, with just 5% employing static code only.

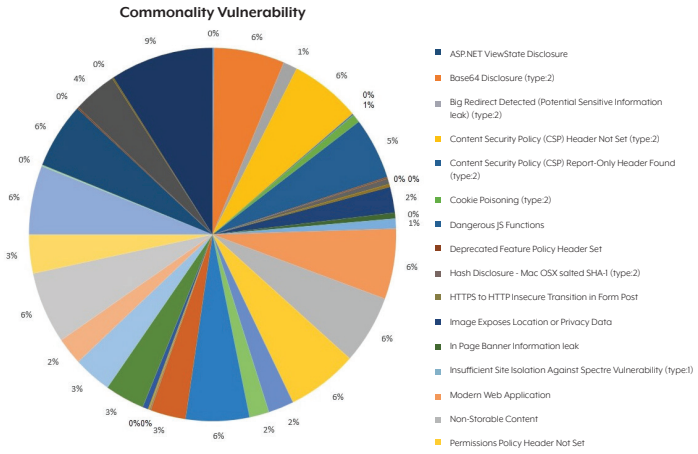
Furthermore, a significant number of sites using a CMS (around 40%), including a significant number of those that are 'household names', were built using WordPress and or WordPress/WooCommerce – completely unremarkable since those platforms dominate the market globally[43], with the next most popular systems failing to capture even collectively even half of the WordPress share.

For that reason alone, a large number of vulnerabilities discovered were related to WordPress customisations, plug-ins and other available resources although no site using any other CMS or alternative solution was free of such issues.

To establish the degree to which these customisations (and plug-ins etc.) can affect a site's cybersecurity, baselines were established by testing out-of-the-box, 'vanilla' installs of each of the below products:

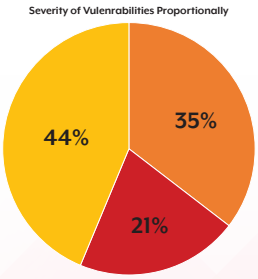
- Wordpress
- Wix
- Squarespace
- Shopify
- Magento
- Joomla
- Drupal
- BigCommerce

The resultant Cyber Tzar scores were in a range between 586 and 775. These results illustrate that cybersecurity attention is warranted even for new installations, primarily due to out-of-date components within install packages and the rapid pace of vulnerability discovery and 'bot' development.

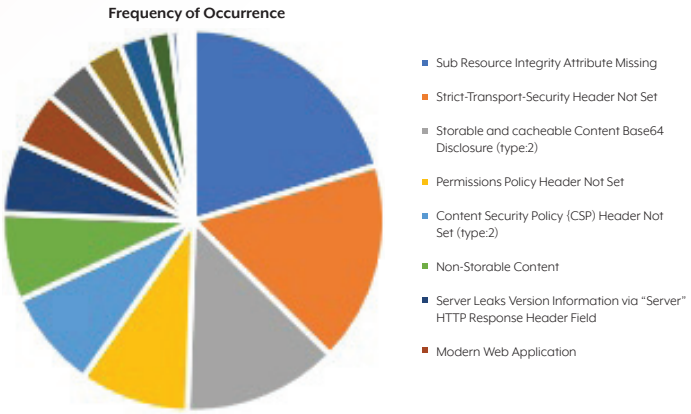


Finally, analysis of vulnerabilities themselves reveals both that a relatively small number of issues account for the majority of problems discovered and that only a fifth of these could be characterised as falling within the 'Red' Risk Group (i.e. those that require immediate remedial action). Of these, the most commonly found were related to outdated JavaScript Libraries,(~ 35% of sites) potential PII Disclosures (~ 40% of sites) and the absence of sub resource integrity attributes (~ 40%), with source code disclosures of various types also appearing regularly.

With that said however, even though 'Red' Risk Group vulnerabilities represent a minority of those discovered overall



While these findings largely point to the need for ongoing and improved website maintenance and hygiene, other matters – for e.g. the absence of sub resource integrity attributes – are issues that clearly need to be considered in the site's development process - as the 2019 discovery of a malicious skimmer on the website NBA.com demonstrated, when attackers altered a JavaScript library to steal credit card information from its customers[44].



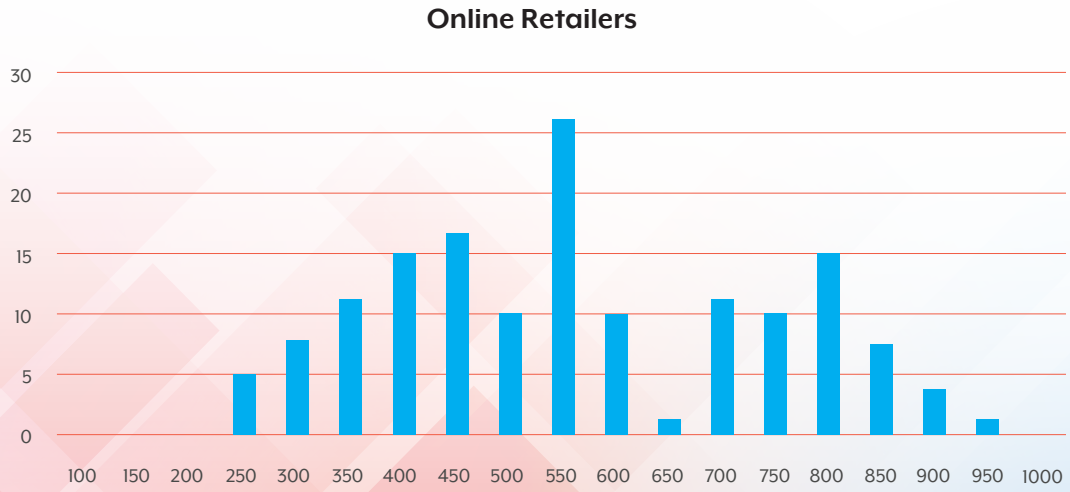
The ubiquity of such issues – some of which can be used to effect any number of common attacks such as injections[45], exploitation through information disclosure[46] etc. - together with the prevalence of webforms to receive email mean many of the sites tested were potentially open to data breaches, cross site scripting or page 'spoofing'[47], which we feel could be undertaken with relative ease in a significant number of cases.

The below subsections, which discuss each of the business sectors we examined, provide only a 'quick glance' at the results and – as mentioned - a further, more detailed technical analysis will form the basis of a subsequent Report.

Online Retailers (Average Score 680)

As Table One indicates and the below graph confirms, this sector represents businesses with the highest score *on average*, and indeed included within it is the most consistently high-scoring site (901) our survey examined – including in regular re-testing over time. Belonging to a high-profile High Street retailer with a brisk e-commerce component, the company employs a full-time, in-house digital team to monitor, test and maintain the site and advised us standards were maintained as follows:

> *'Regular penetration testing across the whole solution and specific pen-tests for any new capabilities that have a material risk-profile. Static code scanning, training of engineers on good practices and a range of opportunities for them to practice these in simulated scenarios; regular risk reviews and audits + an in-house team of security experts that coach and guide the various delivery teams.'*



Clearly, not all online retailers are as able and willing to be as thorough as the above interviewee, although the group did include the second largest proportion of higher scoring sites (32%). Nevertheless, it also comprised a disturbing number of poor or average scoring sites, including among companies and brands that are extremely well-known.

Additionally, a considerable number of sites in this group were worrying since it was clear a high percentage – up to 50% of those examined - were not only vulnerable to various types of cyber-attack but that potential data breaches were quite possible, even likely.

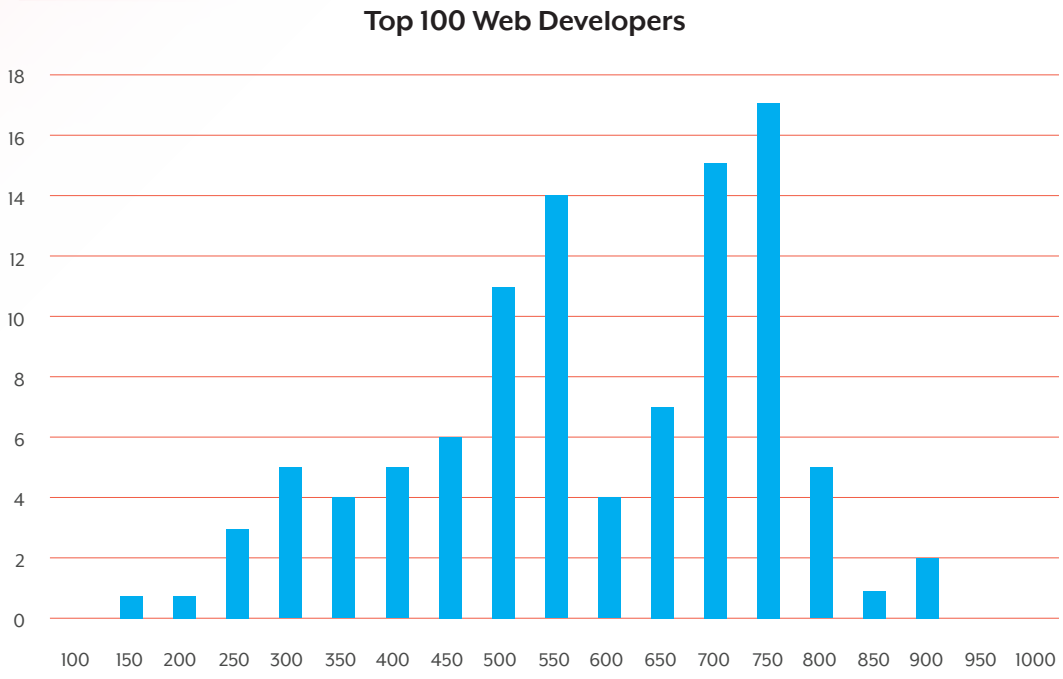
For example, in more than one site, cross site scripting attacks were clearly possible, with easily accomplished cookie capture enabling an attacker/bot to access accounts with vulnerable logins. Another vulnerability discovered – among e-Retailers but also in other groups – were possible JavaScript/HTML exploits which would also enable access via JavasSript manipulation unless other additional security measures were in place.

Interestingly, while exploring this group in greater detail we discovered that both the top scoring site (score 901) and one of the lower, and extremely vulnerable sites (scoring 241) were each built using the Adobe Experience Platform supporting our conjecture that poor cybersecurity performance was *not* linked to delivery software choice while emphasising the need for excellent front- and back-end development plus ongoing site maintenance/hygiene.

Top 100 Web Development Agencies (Average Score 560)

Although scoring lower on average than e-Retail websites, the Top 100 Web Development Agency group had the largest percentage of higher scoring sites (38%) which one might expect from those in the industry whose sites serve as the main shop window for and example of their work quality.

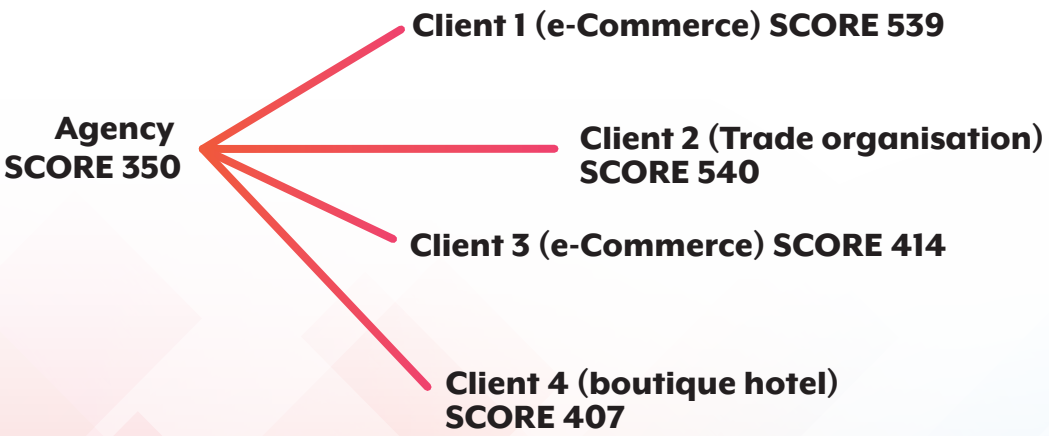
For some among them however, cybersecurity does not appear to be a priority focus.



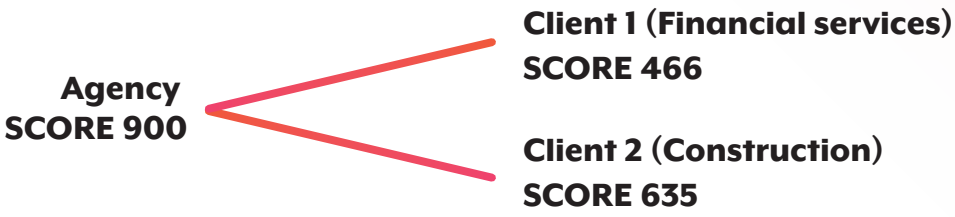
Indeed, as the above graph indicates, at least 25% of the websites among this group were poor where cybersecurity was concerned, some extremely so.

In light of initial findings, we additionally felt it reasonable to try to understand whether any correlation existed between low and high cybersecurity scores of web agency sites and those of their clients.

Here, we discovered that, for low-scoring agency sites there *did* appear to be some correlation in that client sites almost always scored poorly themselves – see the example below:



However, little or no correlation was found between agencies whose own sites scored highly the client sites those agencies had built. In other words, high scoring agencies often had clients some (not all) of whose sites scored relatively poorly – see second example below:



It's important to point out however – based merely on such findings as these – that blame or responsibility for the poor security of client sites cannot necessarily be placed with the web development agency in either of the above two scenarios.

Responsibility for site maintenance, hosting, management etc. may not have been left with the agency and – due to poor practice in these areas outside of the developer's remit – an initially high scoring site may have deteriorated over time unconnected to the agency's own effort.

And while it's of course unfair and inaccurate to generalise about web agency cybersecurity commitment, for businesses or individuals commissioning new projects from any such organisations an attitude of '*caveat emptor*' would certainly apply when seeking to appoint a provider.

Outputs for example might be determined by whether or not the agency concerned employs full-stack developers or, failing that, maintains front-end and back-end developers in-house able to incorporate requisite security measures, themselves assessed via static code testing throughout the development process. Finally, a demonstration of a site's security at a project's completion alongside transparency in respect of routine maintenance processes employed by the agency of both front- and back-ends after the site has gone live would contribute greatly to improving website & web app security. These issues are further discussed in the Addendum at the end of this Report.

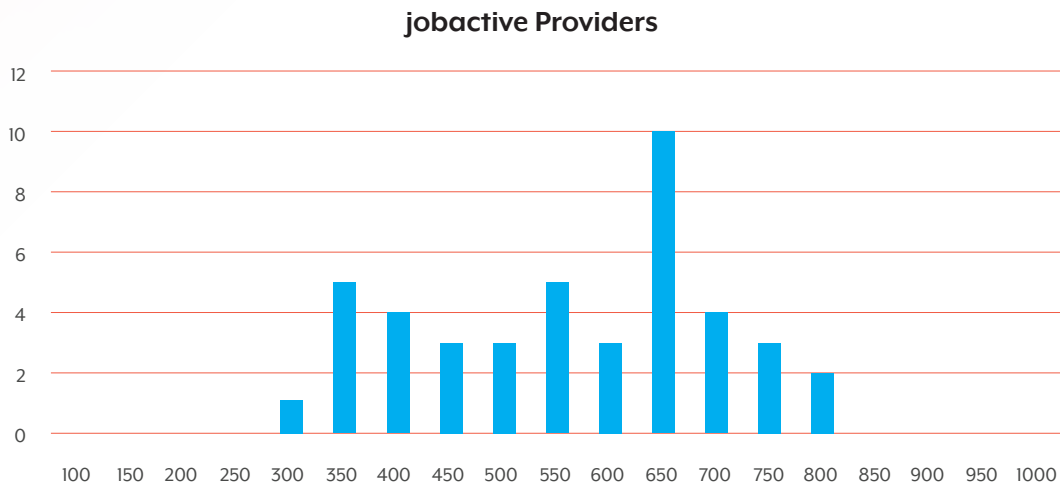
Meanwhile, agencies themselves have a representative body called AWIA (the Australian Web Industry Association)[48] which we approached during writing and which has expressed an interest in reviewing our findings on publication.

jobactive Providers (Average Score 553)

Of the business sectors examined, the 40 jobactive Providers which run and maintain offices and services within multiple locations across Australia on behalf of the Commonwealth Department of Education, Skills and Employment were perhaps the most surprising in that, with specific requirements for assessing data risk, one might have expected a higher standard of web and web application security than was discovered by this survey.

With only ten (25%) of websites achieving what might be described as 'higher scores' and at least ten scoring particularly poorly, we predict much work will be necessary for these organisations to achieve the upcoming 'Right Fit For Risk' (RFFR) stipulation by the Government requiring ISO27001 Information Security Management Certification and a whole-of-business approach to IT security which will inevitably include websites.

No sites were free of vulnerabilities within 'Red' risk groups and outdated coding libraries tended to be the most common problems discovered, suggesting a general lack of adequate site maintenance.



With that said, sites in this group were – with some exceptions - for the most part 'informational' in nature, meaning the results of compromise would be largely reputational. However, in a number of instances, security was particularly poor and consequently may be indicative of a broader lack of cybersecurity understanding.

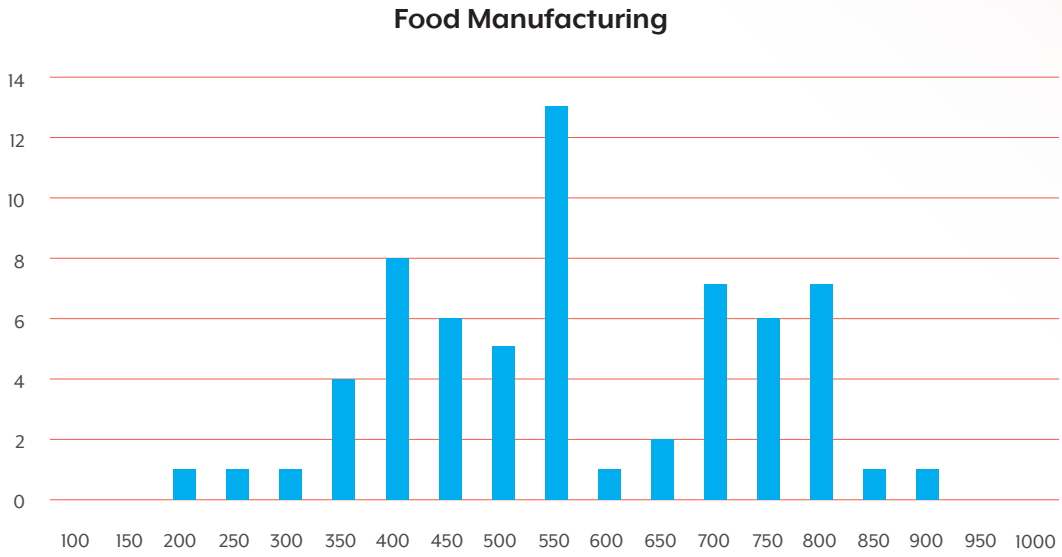
Food Manufacturers (Average Score 549)

Since AustCyber (in 2020) identified manufacturing as a sector at 'high' or 'very high' risk of being subject to a 'cybersecurity shortfall'[49] and recalling the 2021 cyber-attack on JBS Foods after which a $14.2 million ransom was paid[50], food manufacturers seemed an appropriate sector to examine.

While in this group the majority of sites tested (but by no means all) served as little more than 'brochureware' for the company concerned, a successful website/web application attack could nevertheless cause reputational damage even in these cases. Since a sizeable number of the businesses concerned are very well known and their brands of extremely high value, the result of such an attack could therefore be considerable.

As with many – even most – other sites examined, a large number within this group employed webforms to receive email. With some of the vulnerabilities discovered, spoofing these pages, so as to collect information direct from the user, would be possible and, in some cases, easy to effect.

One site especially was of particular concern as log-ins intended for use both by customers and suppliers provided access to various back-end business systems. As well as this, the site's entire directory was visible and overall, highly vulnerable to an attack potentially placing its entire supply chain at risk. Additional sites reviewed had lesser supply chain risks i.e. this was not an isolated instance.



A fairly low proportion of 'high-scoring' sites were evident among the group, especially when measured against some others – for e.g. e-retailers and web developers.

The sector's Peak body, the Australian Food & Grocery Council[51] has been made aware of this research.

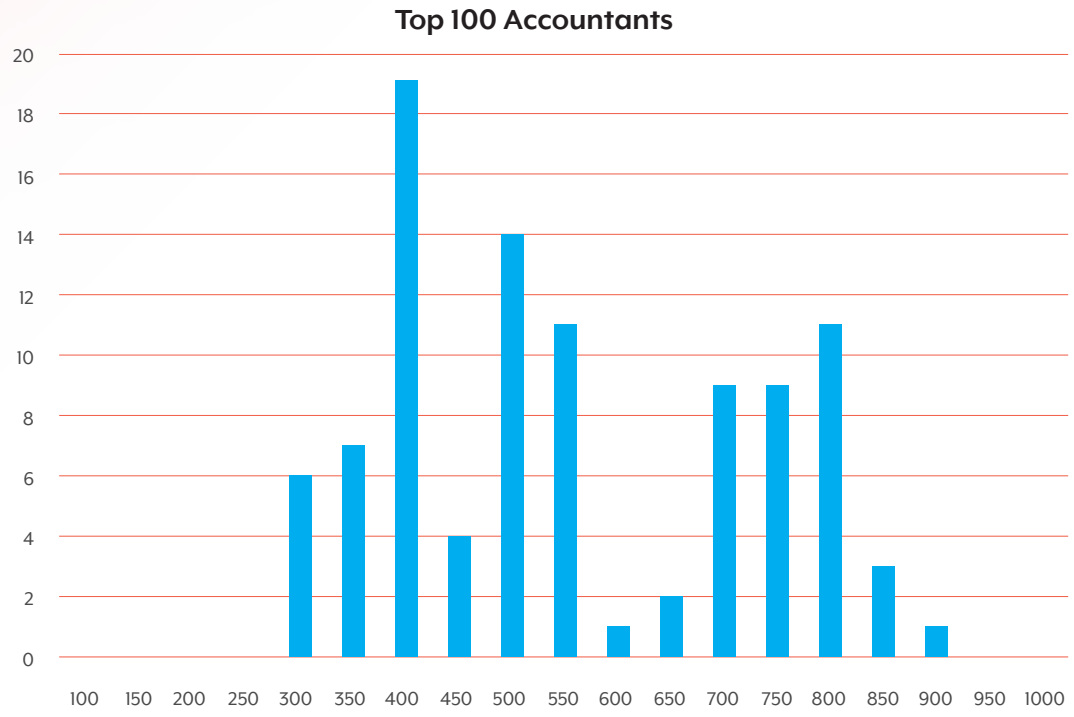
Top 100 Accountancy Firms (Average Score 535)

That the website security scores of Australia's leading accountants were, on average, the third lowest (just above 'local business' and 'charities') of the business sectors we tested was surprising, given the relatively strict regulatory conditions under which they are obliged to operate and the punctiliousness one might associate with the profession.

The AFR's list of 100 top firms covers all tiers of accounting companies, from the Big Four to the relatively small, so resources – including for cybersecurity - will likely vary enormously between organisations.

The above having been said – and while being at pains not to identify any individual company with a particular score – we did find the organisation's size was not always (if at all) correlated with its cybersecurity level; in other words, some of the bigger firms scored fairly poorly.

More generally, as the following graph shows, only around a quarter of sites tested were higher scoring while roughly a third were extremely low-scoring.



As seen in all other sectors, webforms were common among sites within this group, with a number also offering client log-in functionality – including a number which were quite or extremely low-scoring.

The below graphic shows *some* of the issues and their concomitant Risk Groups found in one such example (of a lower scoring site with a client log-in) with numerous instances of very high-risk vulnerabilities - and this example is far from unique.

Vulnerability	Risk Group	False Positive	Count	View
Vulnerable JS Library (type:18)	3	No	1	deta
Vulnerable JS Library (type:129)	3	No	1	deta
Vulnerable JS Library (type:31)	3	No	1	deta
Sub Resource Integrity Attribute Missing	6	No	3	deta
Source Code Disclosure - SQL	8	No	1	deta
Dangerous JS Functions	13	No	2	deta
Content Security Policy (CSP) Header Not Set (type:2)	14	No	87	deta
Permissions Policy Header Not Set	18	No	98	deta
Reverse Tabnabbing	18	No	87	deta
HTTP to HTTPS Insecure Transition in Form Post	18	No	3	

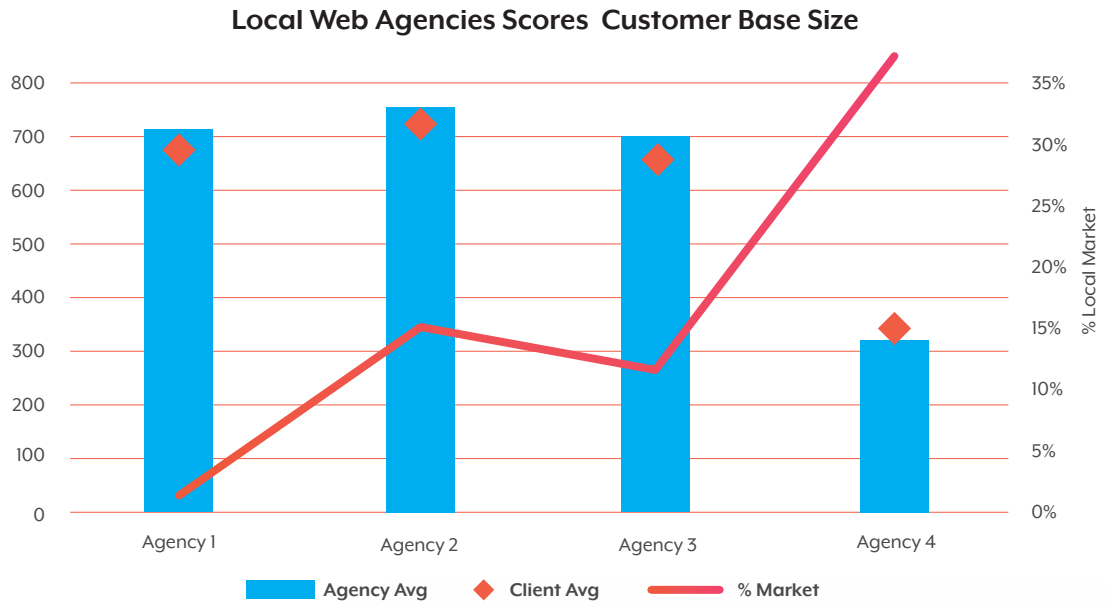
Both main Professional Bodies for accountants/accountancy firms (the CPA[53] and CAANZ[54]) were made aware of this Report's findings, and we note the CAANZ was itself subject to a successful cyber-attack in December 2021[55].

'Local Business' (Central Qld) (Average Score 333)

A modest 'sub-survey' of websites among a limited number (around 30) Central Queensland-based businesses – which included those from the financial and legal sectors among others – was also undertaken during the alpha testing phase of the CyberTzar platform – i.e. from October 2021 onwards. The exercise proved interesting for a number of reasons, not least because it allowed for a series of informal meetings and interviews with various of the business owners concerned.

From the 'local business' sites survey itself however, some notable findings became quickly apparent, these being that:

1. While on average not that much worse than other sectors surveyed, a third of websites scored particularly badly – including those from the financial and legal sectors;
2. Four main web development agencies appeared to be responsible for creating a large proportion of sites constructed locally although one agency appeared very much to dominate the market within this geographical area. Notably, both the agency and clients performed badly where site security was concerned (see graph below).

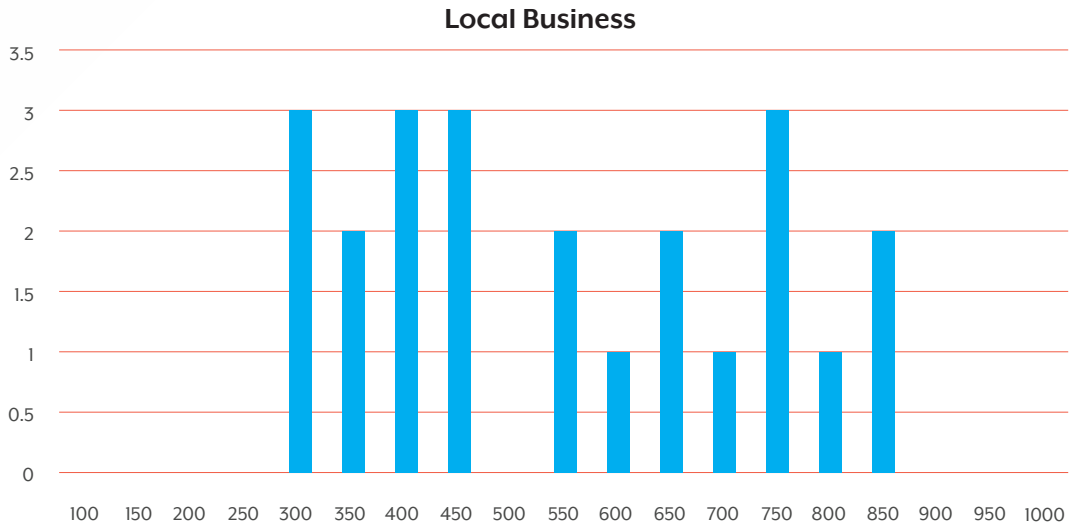


In discussing their website security performance and related matters, some business owners exhibited a poor understanding of IT in general and cybersecurity in particular while some had an ostrich-like reaction to the fact that their websites – including transactional websites - were vulnerable to cyber-attack.

As an example, despite having been victim to such incidents in the past, one business - grown from modest beginnings over three generations into a $multi-million concern today, including through significant online sales - reported leaving '*all that stuff*' (meaning website and IT) to a family member who – though untrained and self-taught – was '*brilliant at computers*'.

In another case, the CEO of a sizeable and growing business in the financial sector, said he '*wasn't interested*' in the fact that the company's website had major exploitable issues.

When questioned about website security, one of the local web development agency owners was unsurprised by the problems discovered but, while acknowledging the importance of updating code libraries and the need for ongoing vigilance, said clients often did not retain his company for such purposes after a project's completion.

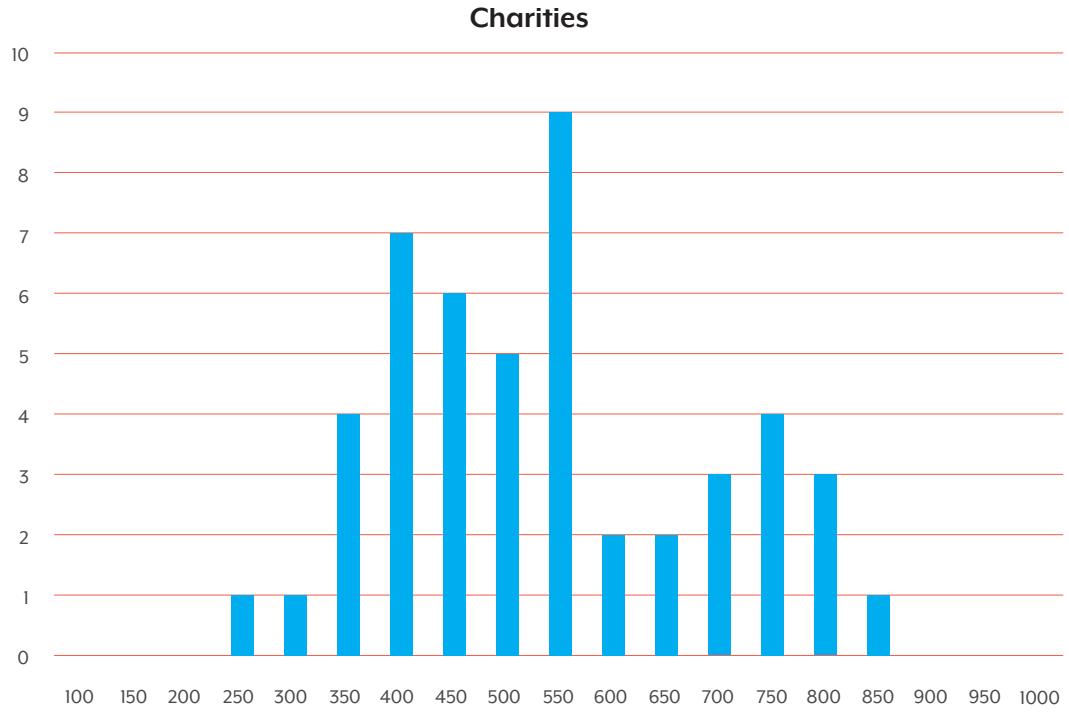


Although it would have been reassuring to find the majority of the 'local' sites tested represented mainly 'brochureware' this unfortunately wasn't the case. About 20% – including hotels, retailers and those from the 'white collar' professions – were to a greater or lesser degree transactional, with the majority (in our opinion) in urgent need of penetration testing. Some were highly vulnerable to extremely serious attack which had the potential to be damaging both to themselves and site users.

Charities (Average Score 522)

Sites tested within this sector represented arguably some of the most worrying of all, not because of the relatively high proportion that scored poorly but due to the fact that almost all – including the most vulnerable - accept online donations.

Commonly found issues (though equally true of all other groups) included vulnerable and/or dangerous JavaScript libraries and functions, source code disclosures, missing sub resource integrity attributes plus many other significant concerns, often throughout entire sites – many belonging to some of Australia's biggest and most high-profile charities.



While each organisation tended to have its own method of receiving online donations – some used (for e.g.) WordPress plug-ins or similar solutions to receive monies directly from their site while others used dynamic means (e.g. linking to third-party providers) – overall the combination of insecure sites and collection of personal and financial information warrants attention.

In respect of where use of third-party providers occur it is impossible to say – on the basis of a static code test alone – whether data, including financial data, is adequately secured and sufficiently immune to cyberattack.

The sector's Peak Body, the Fundraising Institute of Australia[56] was made aware of this Report's findings and is known to be considering the matter.

Conclusions

From the above findings it's clear significant security issues exist across many Australian websites, thus results of Imperva's 2021 Web Application Attacks Survey showing a rapid increase in website/web application attacks[56] is unsurprising.

On a positive note, dramatic improvements to the scenario we discovered could easily and quite cheaply be effected with a small number of relatively simple shifts in approach on the part of site owners and developers, namely by, for e.g.:

- Ensuring sites are adequately maintained, updated and tested;
- Ensuring commonly found vulnerabilities such as missing sub resource integrity attributes are avoided during the development phase;
- Ensuring security is 'written in' to any procurement process and adequately demonstrated before sign-off, along with a clear maintenance plan.

Additionally, in many instances – particularly those within a 'closed' environment such as WordPress - remediation of vulnerabilities, even when occurring in large volume throughout a site, could be undertaken quickly and easily at low cost.

Nevertheless, a high prevalence of some vulnerabilities coupled with the burgeoning use of automated tools ('bots') mean that, unless wholesale action is taken, and taken quickly, successful website and web application cyber-attacks are inevitably going to continue to rise sharply in Australia.

Meanwhile, website security itself suggests something of a gap between what CEO's are *saying* about cybersecurity and what they are actually *doing*.

If PWC's latest CEO survey is to be believed, in which respondents said they felt that, in 2022, 'cybersecurity was of greater concern than the COVID-19 pandemic impacts, economic volatility or climate change'[57], then this anxiety is not generally reflected in the security of a large number of websites.

This report, containing factual site data within and across industries, provides a first basis for benchmarking the intent and actions of Australian businesses in assessing and addressing website-based cybersecurity vulnerabilities. Future reports are anticipated to both deepen the scope of reports, as well as identify trends in website security levels.

For an immediate and free vulnerability test of your website please go to:
https://sentriacyber.com/free-vulnerability-scan

References

[1] See: https://www.abc.net.au/news/2021-10-13/government-will-mandate-business-reporting-ransomware-attacks/100534890

[2] https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21

[3] See: https://www.imperva.com/resources/resource-library/reports/2021-cyberthreat-defense-report/

[4] https://www.cybersecurityconnect.com.au/commercial/7058-web-application-attacks-on-financial-services-up-38

[5] https://cybertzar.com/

[6] https://en.wikipedia.org/wiki/OWASP_ZAP

[7] See: https://themanifest.com/au/web-development/companies (please note: links to 2021 list since the same URL was used when page updated from 2020 to 2021)

[8] https://blog.compliancecouncil.com.au/blog/iso27001-rightfitforrisk

[9] https://en.wikipedia.org/wiki/Cross-site_scripting

[10] See [1]: (https://www.abc.net.au/news/2021-10-13/government-will-mandate-business-reporting-ransomware-attacks/100534890)

[11] https://www.weforum.org/reports/the-global-risks-report-2021

[12] https://www.afr.com/policy/foreign-affairs/more-than-half-of-australian-businesses-disrupted-by-cyber-attacks-20210423-p57lvs#:~:text=More%20than%20half%20of%20Australian%20businesses%20disrupted%20by%20cyber%20attacks,-Max%20MasonSenior&text=Ransomware%20attacks%20shot%20up%20in,security%20firm%20Mimecast%20has%20found

[13] https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21

[14] Ibid.

[15] Ibid.

[16] Ibid.

[17] https://www.austcyber.com/resource/australias-cyber-security-sector-competitiveness-plan-2020

[18] Ibid.

[19] https://www.imperva.com/resources/resource-library/reports/2021-cyberthreat-defense-report/

[20] https://www.infosecurity-magazine.com/news/web-app-attacks-surge-251-in-two/

[21] https://www.cybersecurityconnect.com.au/commercial/7058-web-application-attacks-on-financial-services-up-38

[22] Ibid.

[23] https://www.imperva.com/blog/bad-bot-report-2021-the-pandemic-of-the-internet/

[24] https://en.wikipedia.org/wiki/OWASP_ZAP

[25] https://owasp.org/www-project-top-ten/

[26] https://en.wikipedia.org/wiki/NIST_Special_Publication_800-53

[27] https://attack.mitre.org/

[28] https://en.wikipedia.org/wiki/Risk_matrix

[29] https://www.auda.org.au/

[30] https://www.austcyber.com/resource/australias-cyber-security-sector-competitiveness-plan-2020

[31] https://www.afr.com/companies/professional-services/financial-review-top-100-accounting-firms-2020-20200825-p55p5p

[32] https://insideretail.com.au/tag/top-50-people-in-e-commerce

[33] https://storeleads.app/

[34] https://www.australiancharityguide.org/

[35] https://www.foodanddrinkbusiness.com.au/top-100/exclusive-australia-s-top-100-food-and-drink-companies-2020

[36] https://www.iso.org/isoiec-27001-information-security.html

[37] See: https://blog.compliancecouncil.com.au/blog/iso27001-rightfitforrisk

[38] See: https://themanifest.com/au/web-development/companies (please note: links to 2021 list since the same URL was used when page updated from 2020 to 2021)

[39] https://www.pwc.com.au/ceo-agenda/ceo-survey.html

[40] https://www.pwc.com.au/ceo-agenda/ceo-survey/cyber-top-risk-to-business-growth.html

[41] https://en.wikipedia.org/wiki/Enterprise_resource_planning

[42] https://hackr.io/blog/best-php-frameworks

[43] https://w3techs.com/technologies/details/cm-wordpress

[44] See: https://css-tricks.com/securing-your-website-with-subresource-integrity/

[45] See: https://www.ibm.com/docs/en/snips/4.6.0?topic=categories-injection-attacks

[46] https://www.ibm.com/docs/en/snips/4.6.0?topic=categories-information-disclosure-attacks

[47] https://en.wikipedia.org/wiki/Website_spoofing

[48] https://www.webindustry.org.au/

[49] https://www.austcyber.com/resource/australias-cyber-security-sector-competitiveness-plan-2020

[50] https://www.abc.net.au/news/rural/2021-06-10/jbs-foods-pays-14million-ransom-cyber-attack/100204240

[51] https://www.afgc.org.au/

[52] https://www.cpaaustralia.com.au/

[53] https://www.charteredaccountantsanz.com/

[54] https://www.charteredaccountantsanz.com/news-and-analysis/news/it-incident

[55] https://fia.org.au/

[56] https://www.imperva.com/resources/resource-library/reports/2021-cyberthreat-defense-report/

[57] https://www.pwc.com.au/ceo-agenda/ceo-survey/cyber-top-risk-to-business-growth.htmlv

Addendum

One of the factors identified within the Report was the degree to which Web Development providers were engaged and equipped to provide a secure website 'out-of-the-box' as well as ongoing support for cybersecurity as threats evolved.

In the view of this Report's authors, and observing multiple sites in action across Australia:

- Acceptable to very-good website security can be achieved both with bespoke solutions as well as the use of Content Management Systems (CMS);
- The use of plug-ins within a CMS environment is convenient however may increase the number of potential security openings;
- Regular maintenance appears to be a crucial factor in maintaining security, in particular use of latest libraries and updating similar features as they address known and discovered security issues;
- Regular testing of websites is an essential process for understanding vulnerability, as websites with good security will not remain so as vulnerabilities develop and are exploited.

It's important to restate the results presented in this Report are the result of static code testing, and do not address all possible vulnerabilities. Penetration testing, which simulates human and/or 'bot' activities across the website, will provide a more reliable basis for assessing risk of attack

Selection of a web service provider for development and/or maintenance of websites can also be improved with the following information.

Web development agencies can employ 'full-stack developers', or alternately both 'front-end' (website look and feel) and 'back-end' (website logic and infrastructure) developers. Each aspect of a website has potential for cybersecurity issues, and therefore it is worthwhile discussing with agencies their capabilities and approach to cybersecurity across each domain.