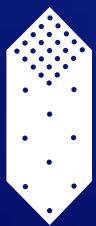


Findings of the 2022–2024 Victorian Government Funded Cyber Security Risk Analysis Project

(Targeted at Small to Medium Businesses)



CITT

Providing Strategic ICT Advice within the Australian
Digital and Telecommunications Industry

CITT Industry Report: Cyber Security Risk Analysis Project



Communications and Information Technology Training Ltd (CITT)

Communications and Information Technology Training Ltd (CITT) is a 'Not for Profit' National Industry company established in 1995 by the Information Technology and Telecommunications (ICT) industries to provide advice and support in implementing ICT workforce strategies and productive skills development. This includes understanding and promoting Government programs, industry employment opportunities and supporting skills training programs in businesses by improving its workforce ICT skill base.

CITT continues to be involved in innovative programs involving technological developments and welcomes all interaction with stakeholders within the ICT sector. Please contact us via our website www.citt.com.au should you have any questions regarding the content of this Industry Report or other matters affecting the sector.

Acknowledgements

CITT would like to acknowledge the key role by Microsoft and National Australia Bank in developing the project implementation process and providing cyber security professionals as Industry Mentors to students.



Industry Report Overview

This report is targeted at Industry Partners, the Education Sector, Cyber Security Stakeholders, Small to Medium Businesses and Government Departments.

CITT (Communications and Information Technology Training Ltd) is a 'not for profit' organisation that provides strategic ICT advice to industry in relation to the digitisation of the IT & Telecommunications industries and undertakes Industry and Government funded projects focussed on training in that market sector. This report provides recommendations and key messages to Industry and stakeholders resulting from the cyber findings of the latest Victorian Government funded project relating to the cyber security posture within the small to medium business sector, and the capabilities of students currently undertaking cyber security qualifications in Victoria.

This report is specifically targeted at industry bodies and stakeholders particularly interested in the cyber security posture of small to medium businesses and those interested in the development of an 'Industry Readiness' capability within newly qualified cyber security cohorts.

CITT would like to acknowledge the key role by Microsoft and National Australia Bank in developing the project implementation process and providing cyber security professionals as Industry Mentors to students.

[Further detail, above and beyond what is contained in this report, may be obtained from CITT directly where appropriate and subject to the confidentiality and privacy agreements established between CITT and the project participants.]

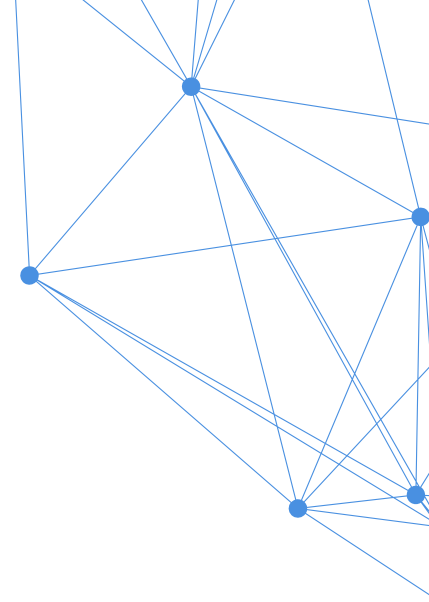
CITT Industry Report: Cyber Security Risk Analysis Project

CONTENTS

1.	Introduction / Purpose of Project	3
2.	Key Recommendations and Messages to Industry and Stakeholders	4
3.	Summary of Project	6
3.1	Approach	6
3.2	Original Concept	7
3.3	The Marketing Message	8
3.4	The Promoted Business Benefits	9
3.5	Time Frames	10
3.6	Project Statistics	11
4.	Detailed Cyber Risk Findings	12
4.1	Cyber Awareness Posture within Small Businesses	12
4.2	Website Configuration Risk Status and Potential Impacts	13
4.3	Process and Procedure Risk Status	14
5.	Education and Training Findings	15
6.	Review Existing Cyber Analysis Tools and Resources	17
7.	Participant Feedback	18
8.	Suggested Strategies for Achieving Ongoing Implementation	20
	Appendix 1: Explanation of Website Configuration Settings	21
	Appendix 2: Process and Procedural Risks	23
	Appendix 3: Contributors to this Report	25

1.

Introduction / Purpose of Project



The Victorian Government funded the CITT Small Business Cyber Security Skills, Risks and Workplace Practices project under the Workplace Training Innovation Fund (WTIF) program. The initiative became generally known as the 'CITT Cyber Security Small Business Risk Analysis Project' in communications between stakeholders. The funding was approved on 8 July 2022 with project implementation completed and final report submitted by 12 July 2024.

Key drivers for the project included addressing:

- A lack of cyber knowledge and skills, with respect to potential threats within small business.
- A perceived limited awareness by small and medium businesses of cyber risk analysis tools, information and services available.
- The impact of current cyber threats and costs on the economy in general and specifically to small businesses which can be catastrophic from a financial, operational and security / integrity perspective.
- Industry concerns in general about the need for more practical skill development and experience amongst learners prior to seeking employment.
- The desire of Microsoft and National Australia Bank to support learners with highly qualified Cyber Security Professionals as Industry Mentors as part of their corporate citizenship initiatives.

Major outcomes were:

- Explaining cyber jargon and terminology to small business representatives.
- A final Report identifying specific business website configuration of cyber risk vulnerabilities including providing advice and recommendations on process and procedural practices that should be adopted or improved within the business.
- Providing businesses with information on the specific consequences of any existing risks.
- Providing learner experience in interacting with real world businesses and explaining technical issues in common language.
- Learner increased confidence in communication, interviewing, presentation, investigative and discovery skills, and application of learnings.
- Building professional networks between learners, TAFE personnel and Industry Mentors.
- Reaffirming and dimensioning the cyber risk posture of small business within the community.
- Providing small businesses with links to access cyber security on line information and support.

Microsoft Media Release: [Click Here](#)

2.

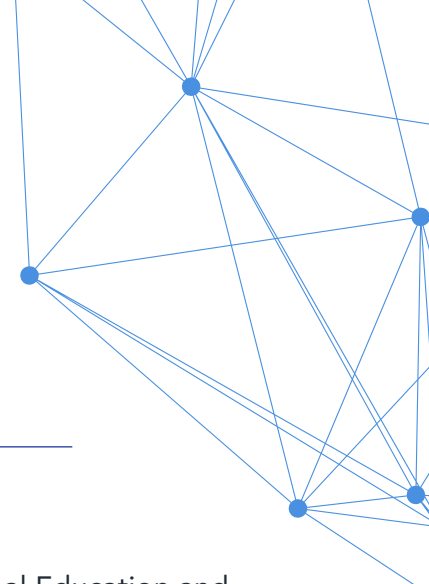
Key Recommendations and Messages to Industry and Stakeholders



- In general it was found that medium (and presumably larger) businesses that have either access to internal IT support capabilities, or a budget that enables ongoing external IT support services did not see a need to engage in this project as they felt their cyber risks were being adequately addressed already. This is an unfortunate perception which may explain why so many threat attempts are successful. As business websites (and email communications) are usually the main access points between internet activity and business operations the project focussed on how vulnerable the website primary configurations were compared to international standard, ISO 27001.
- The analysis carried out under this project's scope was designed to raise awareness within small to medium businesses only, but additionally provided recommendations on website configuration settings and internal business processes and procedures. The conversational nature of the interaction with business we believe made a huge difference in getting the message across regarding the risks, the meaning of terminology in layman's terms and the ease with which remedial action can be taken.
- Had there been greater resource availability, the tool used could have also tested risks in email and content management system configurations. All of these tests are non-intrusive and do not require direct involvement of the business personnel and take only a matter of minutes to obtain results.
- Based on the above it would be possible to carry out a much broader analysis of risks across all industries with the possibility of making it incumbent on service providers such as Domain Name Registrars and Web Hosting Service Providers to implement appropriate configuration setting standards rather than leaving it to the customer.
- A level of 'Cyber Support Expertise' services would be valuable at a more local level where specific analysis of current risks and threats could be carried out at low cost and solutions actually implemented. It would also be better received by businesses if a conversation could be had with an expert rather than a 'bot' or 'chat' engagement.
- Many participating businesses were either overwhelmed by the amount of information available on cyber threats and recommended actions or alternatively had no idea where to find it as much of it is buried in websites

2.

Key Recommendations and Messages to Industry and Stakeholders (cont.)



that often cannot be located using the search function on the home page. It would be worthwhile for one specific location to be nominated as the ideal source of all the highly regarded cyber security awareness documentation, analysis tools and advice from all areas such as Microsoft, the Banking Sector, Industry bodies, Government Departments, Internet Service Providers, Security Agencies etc. At the moment a search may well lead you to many commercially motivated sources anywhere in the world... and who knows perhaps even hackers / actors themselves seeking to get access to potentially vulnerable targets.

- IT was extremely difficult initially for the project team to find 'non-commercially driven' analysis tools that were reliable in terms of the quality of the output report content and availability in time of need. It would be of significant value to have a tool such as .auCHECK reinstated, and made known to be available to small business and IT service providers as a legitimate method of doing simple and reliable tests to improve website security.
- Most businesses were initially uncertain of the value to be gained from this project due in part because the analysis team was made up of current cyber security students (supported by cyber security professionals as Industry Mentors). The resulting response at the completion of the analysis however was one of heightened appreciation. There is much greater scope for engagement

between the Vocational Education and Training (VET) sector and local businesses on the basis of mutual benefit but it needs to start on a small scale such as this project provided (two 1 hour engagement sessions) in order for the confidence and understanding of benefits to be gained by the parties and positive benefits to be recognised. Due to the nature of small business pressures of limited time, funding and resources it was extremely difficult to gain the required level of engagement even for a project of this relatively small size.

Further and improved cyber support can be provided to small business by incorporating this project into ongoing TAFE course delivery and creating local centres of expertise for advice, analysis, rectification and ongoing support.

3.

Summary of Project



3.1 Approach

A process for delivering the project was developed in conjunction with the six participating Victorian TAFE educational bodies: Chisholm TAFE, Kangan TAFE, Holmesglen TAFE, Melbourne Polytechnic, Swinburne University and Victoria University. The detailed scope was defined but some key criteria determined by CITT and the TAFE Community of Practice such as:

- Non-invasive risk analysis activity with minimal intervention and no risk to the business day-to-day operations.
 - Analysis tools used to be sourced from reliable non-commercial sources that can be utilised by businesses in future.
 - Learners to be encouraged to volunteer for participation as this was not part of their cyber security curriculum.
 - Analytical and technical tools to be aimed at learners who are at a suitable stage and level in their course.
 - Marketing promotion to be aimed at small to medium businesses from various industries and geographical locations within Victoria.
 - Ensure learners are at a suitable stage and level in their course to understand the analysis tools and the technical aspects of the reports generated.
- Industry Mentors to have a quality control role in reviewing accuracy and alignment of the content of the final reports to the specific business.
 - Analysis activities and interactions with the business to be able to be performed remotely.

The program commenced with a one day workshop for each group of learners who were divided into teams of two or three students per business. During the workshop the process and activities were discussed in detail including familiarisation with the chosen analysis tools and initial discovery of the allocated business.

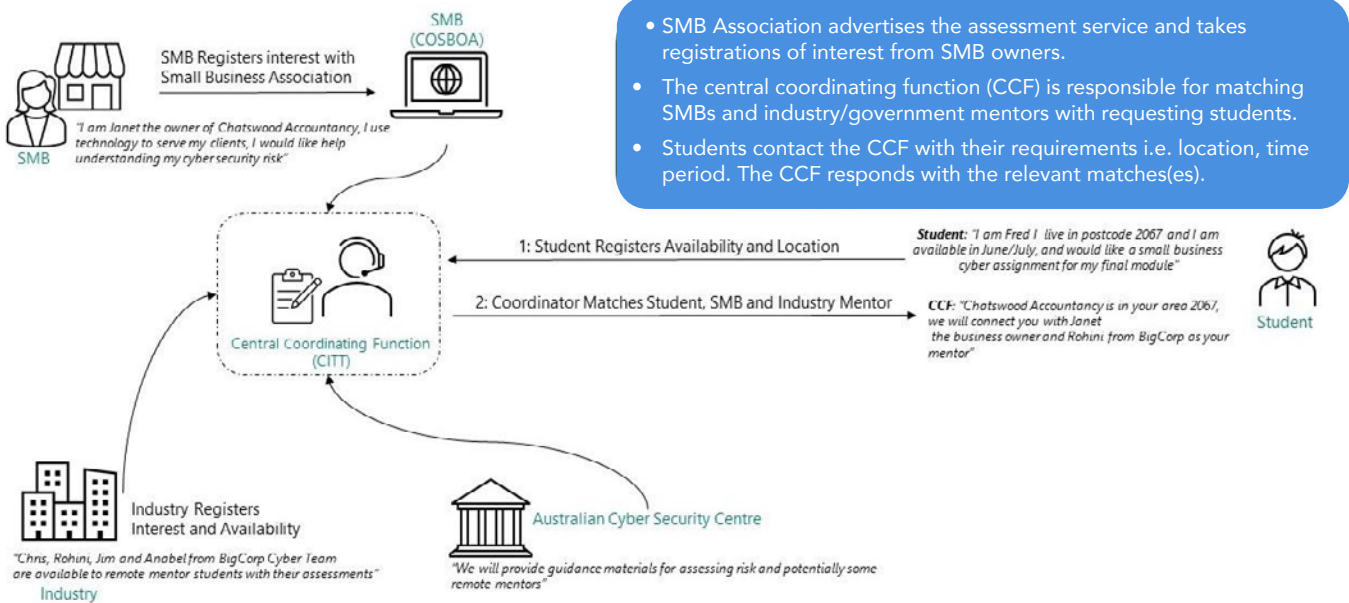
138 Learners from the six Institutions, 52 small businesses, and 16 Cyber Professionals as Industry Mentors participated in the project support.

3.

Summary of Project (cont.)

3.2 Original Concept

The original Microsoft concept model below was implemented with a number of variations due to limited resource availability within stakeholder groups. The final approach did however substantively satisfy the original intention and desired outcomes of the concept.



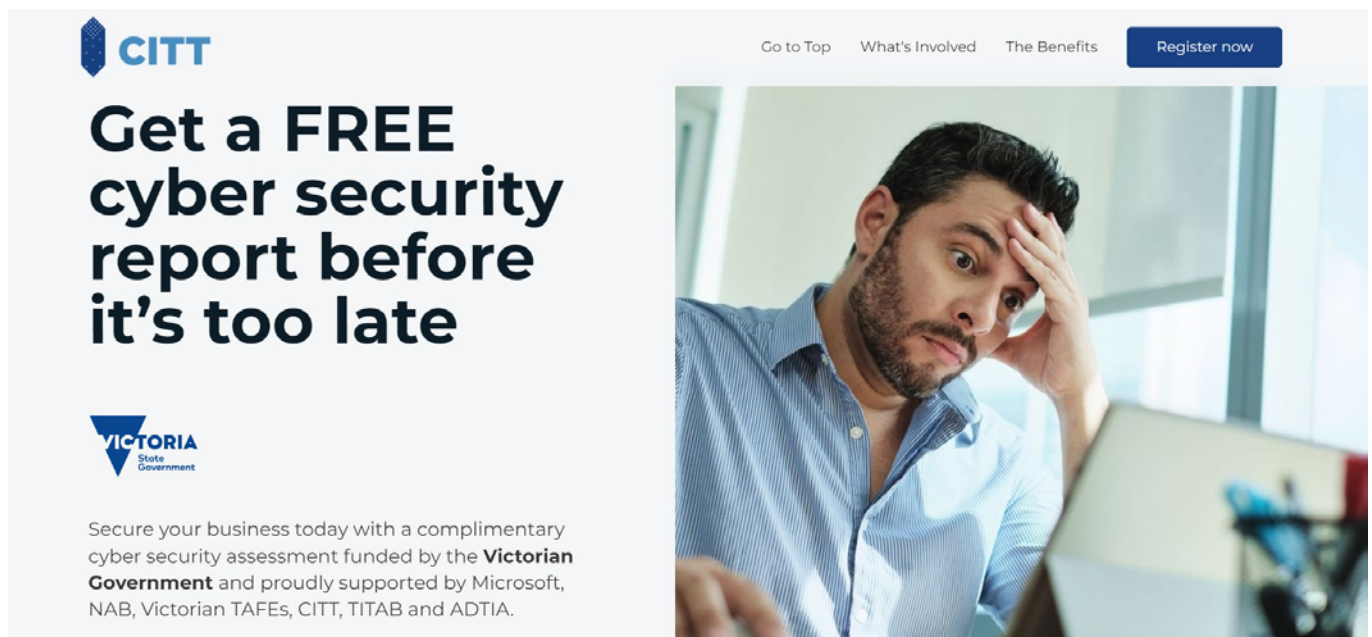
Original concept principles were adopted and modified to suit resource availability and learner practicalities.

3.

Summary of Project (cont.)

3.3 The Marketing Message

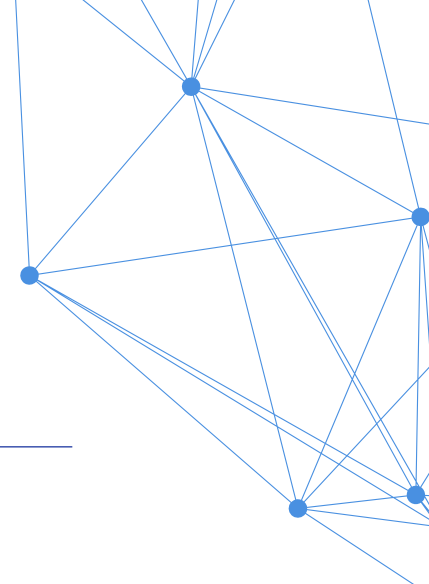
A marketing campaign was developed to encourage businesses to take up the offer as explained in the image below. These resources were distributed via various channels such as email, local council business forums, newspapers, industry bodies and google ads.



The image shows a screenshot of a website landing page. On the left, the CITT logo is displayed above the headline "Get a FREE cyber security report before it's too late". Below the headline is the Victorian State Government logo and a paragraph of text: "Secure your business today with a complimentary cyber security assessment funded by the Victorian Government and proudly supported by Microsoft, NAB, Victorian TAFEs, CITT, TITAB and ADTIA." On the right, there is a navigation menu with links for "Go to Top", "What's Involved", "The Benefits", and a prominent blue "Register now" button. Below the navigation is a photograph of a man in a blue shirt looking stressed, with his hand on his forehead, sitting at a desk with a laptop.

3.

Summary of Project (cont.)



3.4 The Promoted Business Benefits

A landing page was developed to simplify the previous manual process of registration for the service by small to medium business representatives. The benefits promoted were outlined in the image below.

Reduce your risk of cyber attack



- **Identify Risks Quickly**
Identify potential threats and vulnerabilities that could compromise your business's digital integrity.
- **Prioritise Threat Severity**
Understand the severity of each threat, enabling you to prioritise and allocate resources effectively for optimal protection.
- **Tailored Recommendations Provided**
Receive personalised recommendations to address identified vulnerabilities and strengthen your security protocols.
- **Proactive Protection Roadmap**
Access a clear roadmap for proactive measures, ensuring robust protection against emerging cyber threats.

3.

Summary of Project (cont.)

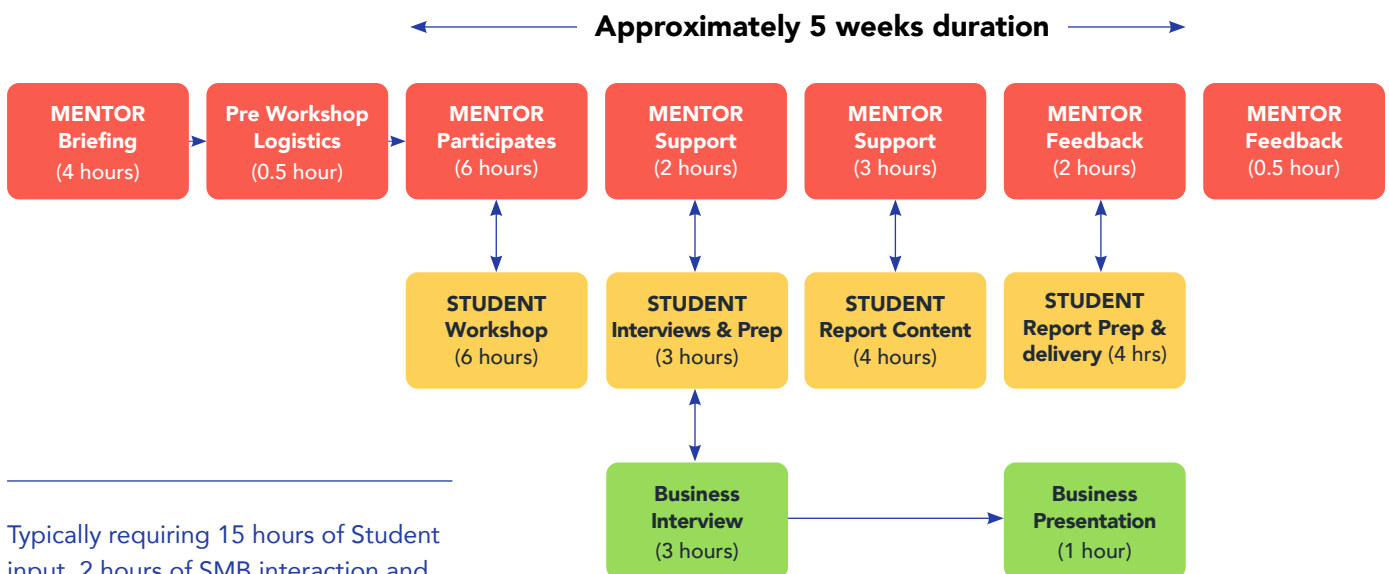
3.5 Time Frames

- The implementation of the project involved approximately 12 months of development of the processes to be used and supporting materials in the forms of kits for each of: TAFE co-ordinator, Learner (Student) and Industry Mentor.
- Also engagement and agreements needed to be reached with each eligible TAFE Educational Institution, liability concerns resolved, and Expressions of Interest covering off confidentiality matters and transparency of process to allay any fears of analysis activity impacts on the business.

- The remaining 12 months covered the running of a pilot program to review and improve processes and documentation then the roll out of a further 14 programs across the six educational institutions.

Remote risk analysis with minimal distraction for businesses and opportunity for direct interaction between Industry Mentors, Students and Business Representatives.

The typical roll out at each institution was as follows:



Typically requiring 15 hours of Student input, 2 hours of SMB interaction and between 18 and 25 hours of Mentor input depending on number of student teams mentored.

3.

Summary of Project (cont.)

3.6 Project Statistics

Statistics Totals for Workshops							
Summary for Toatal Program							
TAFES	6						
Workshops	15						
Mentors Total (Indep / NAB / Micr)	16 (3/11/2)						
Students Total (M / F)	138 (105 / 33)						
SMBs (4 Partial Completion)	52						
TAFE Breakdown:							
		Chisholm	Holmesglen	Melb Poly	Kangan	Vic Uni	Swinburne
Number of workshops		4	2	2	2	2	3
Number of Businesses / Teams		10	8	10	4	9	11
Students (Cert IV)		25	13	28	11	21	32
Students (Adv Diploma)			8				
Statistics for Businesses							
Statistics for Businesses		Business Lcations					
Industry	No of SMBs						
Construction & Maintenance	12						
HR Services	3						
Marketing	5						
Retail	4						
Hospitality	2						
ICT	11						
Hairdressing	4						
Education	4						
Health	1						
Security	1						
Financial Services	2						
Govt Services	3	Central	North	East	South East	West	Country
Total Businesses	52	13	4	17	2	11	5

Businesses from a broad range of industries with different business operations and locations engaged with the six Training Organisations.

4.

Detailed Cyber Risk Findings

4.1 Cyber Awareness Posture within Small Businesses

One of the main objectives of the project was to raise awareness of small businesses to cyber security risks, impacts, remedial actions and available information and assistance. In order to ensure the awareness and learnings were relevant, it was decided to use tools that could identify specific risks to the individual business.

In developing a final report which was presented to the business representative, the analysis teams carried out discovery of: the business activities, the related industry, the business exposure – through a variety of social media platforms as well other service providers such as linkedIn, Google search etc. The process then involved analysing the website, and discussing processes and procedures with the business representative and pitching the findings and recommendations appropriately for the current level of awareness.

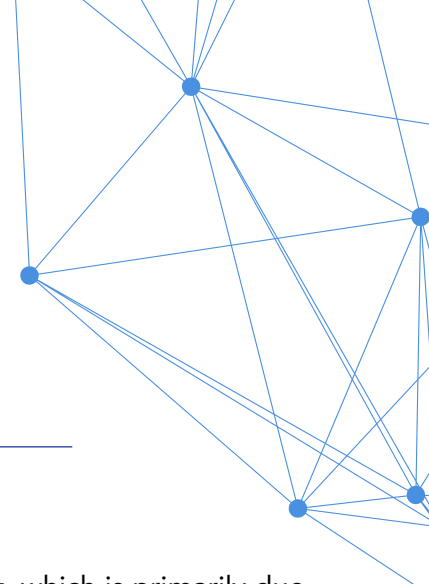
Limited knowledge and skills were evident in the small business cohort so the awareness aspects of the project were greatly appreciated.

In general, the observations of the businesses who registered to participate in the analysis were:

- The project validated that time availability and perception of costs were the biggest inhibitors to any small business keeping on top of cyber risk management.
- None were aware of the analysis tools we had utilised for the activity even though they were readily available on government websites.
- Some believed that whilst their website link had https// they were automatically very secure.
- Most had some idea but very few had a sound knowledge of processes and procedures that should be implemented to improve security.
- Very few had good technical knowledge of website configurations, risks and management. In many cases they did not know who their service providers were (such as web host or domain name provider) and often had no regular IT support arrangements.
- The project validated that time availability and perception of costs were the biggest inhibitors to any small business keeping on top of cyber risk management.
- Medium sized businesses with internal IT support did not participate when approached as they believed they had everything adequately under control.

4.

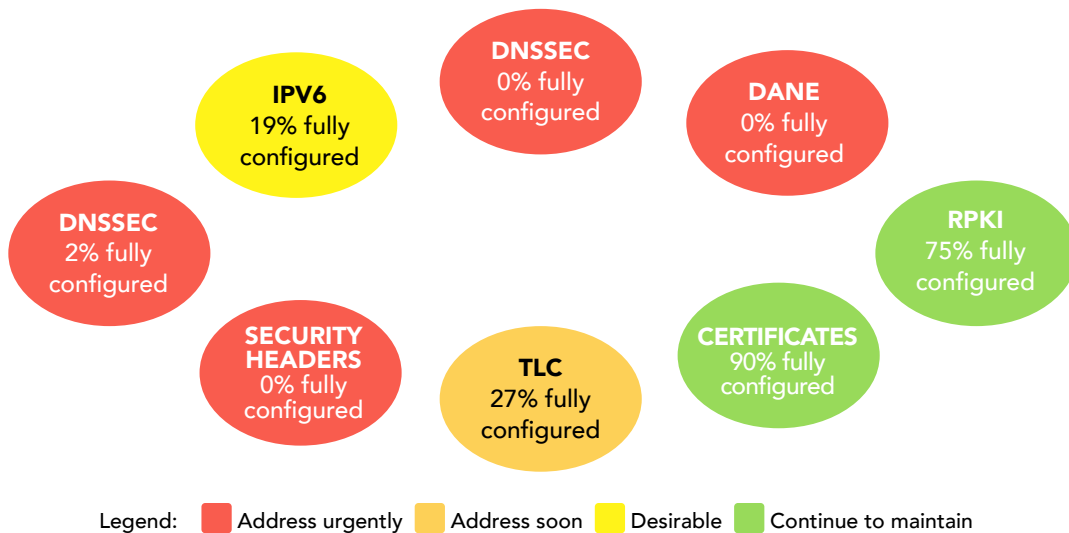
Detailed Cyber Risk Findings (cont.)



4.2 Website Configuration Risk Status and Potential Impacts

As a business website is virtually a window to the internet world and also into the business, it may well be the initial target of any interrogation by hackers / actors. One of the analysis tools specifically looked at website configuration settings and compared them to international standards. In summary, the picture looked much less than optimal. The results below indicate the percentage of businesses participating in the project that had fully configured each of these settings. Appendix 1 gives a more detailed explanation of what each setting contributes to reducing cyber threats.

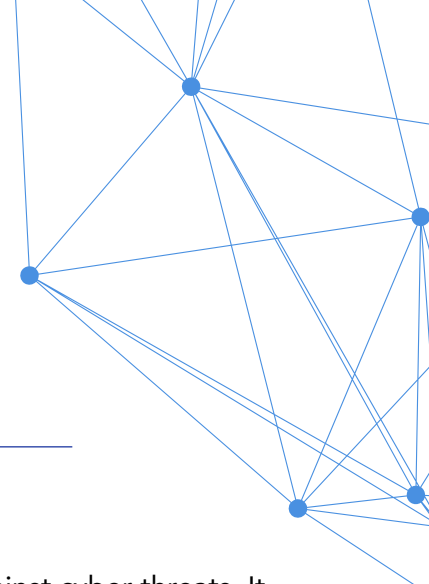
Apart from the IPV6 result, which is primarily due to Australian internet service providers not yet fully implementing IPV6 as standard, the other results show weaknesses that can be fixed quite simply but do require coordination between various service providers such as web hosting, domain name registrars etc. It is important to also note that the assumption that as long as your website URL shows 'https' it is secure, could hide the fact that not all necessary settings have been implemented. To be secure to a level of best practice, there are further settings not shown in the diagram that also need to be addressed. Some of the potential threats that can be avoided by fixing the configuration settings are shown in Appendix 1 to this report.



Website configuration settings pose a considerable risk to business, customers and suppliers.

4.

Detailed Cyber Risk Findings (cont.)

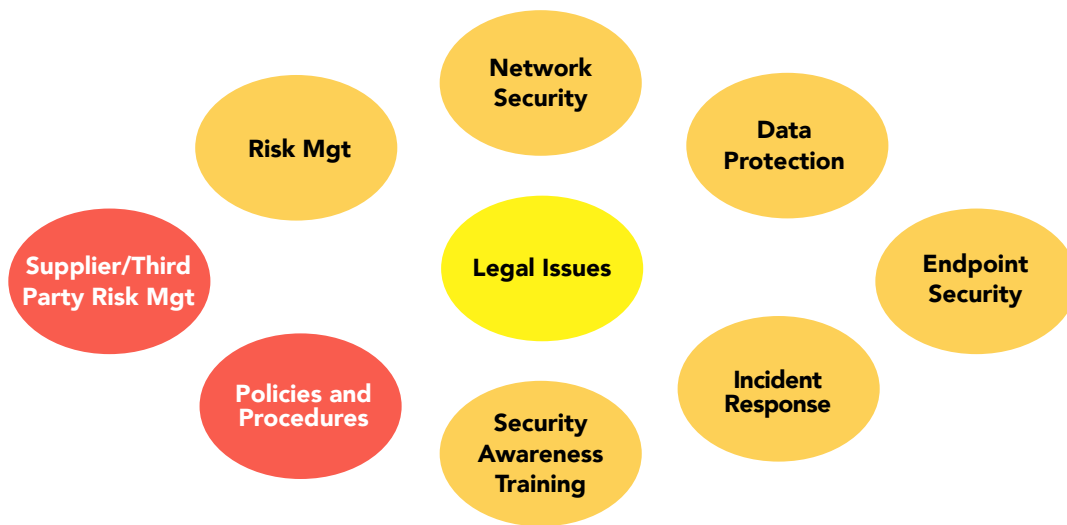


4.3 Process and Procedure Risk Status

The Cyber Security Assessment Tool (CSAT) hosted by business.gov.au is a very good free online resource designed to help businesses assess their current level of cyber security readiness. It provides a series of questions and prompts across various areas of cyber security, such as data protection, network security, and employee training. The CSAT aims to raise awareness about cyber security risks and encourage businesses to take proactive measures

to protect themselves against cyber threats. It also offers recommendations and resources for improving cyber security posture based on the assessment results. This tool provides a general perspective of cyber risk and so added value to the project was contributed by tailoring the questions to the specific businesses involved.

Here's an overview of the specific risk areas discussed and the more detailed findings can be found in Appendix 2 of this report.



Legend: ■ Address urgently ■ Address soon ■ Desirable ■ Continue to maintain

Weak processes and procedures pose a considerable cyber risk to business, customers and suppliers.

5.

Education and Training Findings

Learner Eligibility: Content of current courses in cyber security were reviewed with assistance from the TAFE Community of Practice to determine the appropriate level of learner technical skills that would ensure they could utilise the selected analysis tools and understand the respective output reports. Any learners who had completed the first semester of Certificate IV in Cyber Security or enrolled in Advanced Diploma in Cyber Security were eligible.

Motivation: On the successful completion of the analysis activities and verification by Industry Mentors that all students participated in the team activities, students were awarded with an Industry Certificate endorsed by the TAFE, NAB, Microsoft, CITT and the Victorian Government. This was greatly appreciated by students as an additional input to their resume and validation that they had some experience in dealing with industry on addressing cyber

issues. As a thank you and to acknowledge that the project activity demanded additional student time of approximately 15 to 20 hours outside the cyber security TAFE course, successful student participants were also provided with a participation e-voucher.

Learner Benefits: The students were extremely appreciative of both the face-to-face and then online interaction with the NAB and Microsoft cyber security professionals acting as Industry Mentors. The mentors not only supported the students throughout the project but also provided anecdotal information on potential career paths and an understanding of the real world cyber environment in large organisations.

Many benefits were achieved for Learners, Industry Mentors and Educational Institutions.

5.

Education and Training Findings (cont.)



Industry Readiness: A detailed analysis and follow up with each student participant would be required to determine the level of contribution this project has made towards students subsequently obtaining employment. However, there is anecdotal evidence that it certainly increased students level of confidence, enhanced quality of resumes and provided a focus for discussions in interviews. As an example there is a case study of a Chisholm student located at: <https://www.chisholm.edu.au/students/student-stories/ict/nitika-lakra>

Professional Networking: In some cases the relationships between Industry Mentors and students provided the students with a potential source of a personal reference for job seeking. This was a voluntary arrangement managed by the Industry Mentors themselves.

TAFE / Industry Relationships: Some of the Industry Mentors indicated a desire to establish an ongoing relationship with the TAFEs as either guest speakers or sessional teachers which would greatly benefit future TAFE marketing initiatives and provide options for continuing a similar program into the future. TAFEs also gained additional exposure within the local business community.

Industry Mentors: All Industry Mentors agreed the experience provided a great deal of satisfaction and opportunity to make a difference to small business cyber safety as indicated by the feedback survey responses.

6.

Review Existing Cyber Analysis Tools and Resources

In carrying out a cyber risk analysis it was preferable to utilise simple tools that would also be targeted for use by the businesses themselves. One of the desired outcomes of this project is to increase the 'awareness' of small business to cyber threats and hopefully provide tools, processes or ongoing support for them to be able to carry out their own future risks analysis activities. This project supported businesses in taking that first step to embracing cyber security risk assessment as part of their normal management function. Feedback received from businesses indicated some of the reasons for the difficulty in getting uptake in the use of cyber risk analysis tools are:

Awareness: Businesses we have talked to are not generally aware of the tools and support services available to them to assist in dealing with cyber security risks. Small business owners do not browse the internet and government websites to

find out what can be done and what is available, in any event even if they did spend time doing this they would also be bombarded with commercially available options. Even the tools we utilised for this project were hard to locate... often nested far down within a website and not locatable via the search function.

Complexity: Many tools require a level of IT or Cyber Security skills and knowledge to understand what the tools are doing and what the output reports actually mean.

Time: If a business does not have a dedicated IT resource or even just someone with a basic IT knowledge available, the 'priority' of doing any level of risk analysis will be low due to the many other mandatory demands already placed on businesses.

Perceived Cost: A worry that the analysis will result in the need to engage costly IT expertise to mitigate the risks and additional Software / Hardware.

Motivation: Some businesses indicated their approach will be to fix cyber risk threats as problems actually eventuate i.e. a reactive approach rather than proactive... driven by some of the reasons above. A general belief that if their laptops or systems are hacked, as long as they have a back-up of data, they will just go and buy a new laptop and load the backup on it. A naive view based on experience with viruses.

Existing risk analysis tools and the huge amount of information available to small businesses can be difficult to find amongst commercial / marketing info and somewhat overwhelming.

7.

Participant Feedback

Very positive and complementary feedback has been received from all participant cohorts. Minor negative comments relate mostly with respect to learners' soft skills such as arranging meeting times, presentation skills and converting cyber risk technical data into 'business language'. This is consistent with many cross-industry concerns relating to shortages in soft skills of qualified students seeking work. In the vast majority of cases, participants had indicated the project was extremely beneficial. Later in this document there is a more detailed summary of the feedback received throughout the project. There were well over 100 feedback survey responses captured and the individual comments below are a typical subset.

Business 1 (CITT Member Organisation)

"Understanding the vulnerabilities in our systems, from a third party perspective is so invaluable to us and has given us a clear way forward to address the shortfalls."

Business 2 (Hairdresser)

"As a small business we do not have the capacity to employ IT specialists, everything is managed in-house. Given the recent data security breaches this was a big concern for us. It was reassuring to hear we are on a good path and to get some clear actionable steps we can take to continue offering our clients data security."

Business 3 (Restaurant)

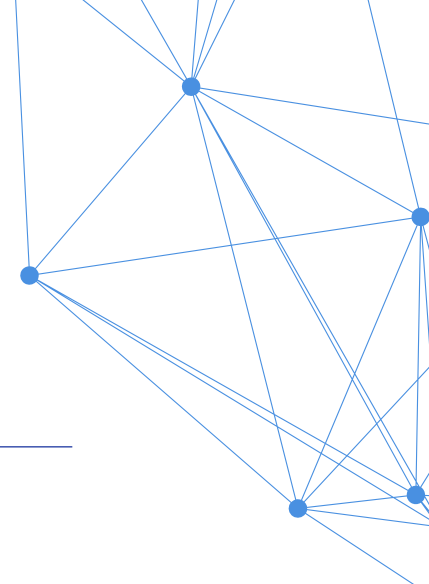
"The interaction with my risk analysis was very positive. Their approach was very clear and relatable to my business. The post analysis was informative and enabled me to look at how cyber security can be better utilised within my business."

Business 4 (HR Resources)

"As a small business, it's often a case of which fire needs putting out now and cyber security is one of those things that you know is important, but gets put to the bottom of the list. It's also an area that is completely overwhelming for a non-tech person – another reason to ignore its importance. This process and the report that I was taken through makes it far easier to understand and also provides a checklist that I can work through to protect our business. It has also given me a level of comfort that we are performing relatively well while highlighting the areas for improvement."

7.

Participant Feedback (cont.)



Student 1

"I gained more knowledge on how real organisation's approach website security and internal processes/practices and gained lots of valuable insight... as they engaged with us well."

Student 2

"I gained the experience of actually doing a project for a real life customer about their cyber safety which will be beneficial for my resume."

Student 3

"A confident boost to speak up and engage with businesses. I am a bit shy when it comes to talking to new people. But with this experience I did the one-on-one questionnaire with businesses rep and then did the presentation about tool 2 assessment report which gave me confidence for the future. Thank you so much guys if it wasn't for you I wouldn't get the chance to have this experience."

Industry Mentor 1

"Team did well identifying the risks of each and communicating this to the business, much of my effort was reducing verbosity and refining business speak."

Industry Mentor 2

"The students all did a great job with the tools and being able to break down their outputs into an understandable format for the SMBs."

Industry Mentor 3

"My team was very enthusiastic and keen to learn and complete the project with the customer. They were very open to my feedback and made changes as per my recommendation. One of the students out of the whole team was very good. He did all the hard work in preparing the presentation and taking the customer through the recommendations. Very well executed presentation."

**Extremely positive feedback
from all participant cohorts.**

8.

Suggested Strategies for Achieving Ongoing Implementation

Currently participating TAFE Educational Institutions have a desire to continue the program into future learner programs, but have limited resource availability to do so. The project materials can be made available for that purpose and CITT could support the Institutions with advice and guidance. Some of the main obstacles to overcome would be:

- Engagement of businesses which may be assisted by greater engagement with Jobs Centres and the utilisation of existing platforms such as Summer Tech Live.
- Greater exposure of the program through TAFE engagement and presentations at Chambers of Commerce and other Council or Industry-based organisations in the local area.
- The ability of TAFEs to provide advice and support to local business without fear of liability risks.

- By mapping and incorporating this program into the course curriculum, the level of input required of the Industry Mentors can be reduced significantly to say 4 to 6 hours per class of students with attendance at the TAFE during normal class hours.
- By initial agreement with the business, websites could be assessed initially and a report prepared for business as a first step (no direct interaction with business initially) to encourage them to get further interested / involved and provide greater access to the business representative. The analysis could then be extended to email set up and CMS (Content Management Systems) without increasing the risk to business.
- Build ongoing relationships between TAFEs and Industry Mentors. Some Industry Mentors in this project indicated they would be happy to provide ongoing assistance to a particular TAFE (convenience of being close to home or work).
- Streamline the Industry Mentor engagement... Could be reduced to maybe two or three 2 hour visits to a TAFE to address a full class of students perhaps looking at three or four businesses in total. One visit as introduction and to advise students on the business 'Discovery' exercise and initial findings of the website analysis tool, the second visit could be to review the outputs of the customer questionnaire / conversation, and if of value, a final visit to discuss the approach of presenting the final results to the specific business.

Further and improved cyber support can be provided to small business by incorporating this project into course delivery and creating local centres of expertise for advice, analysis and ongoing support.



Appendix 1.

Explanation of Website Configuration Settings

IPv6: Internet Protocol Version 6 is an upgraded addressing scheme that offers better security and allows more devices to connect online. The lack of take up by internet service providers at this stage is not seen as a major issue but being ahead of the game in this regard would be good preparation for the future. Along with IPv6 comes a range of additional security measures above the capability of IPv4.

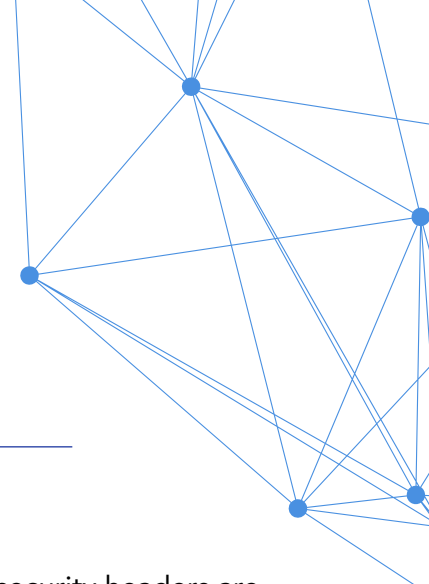
DNSSEC: Domain Name System Security Extensions brings crucial security enhancements to the DNS infrastructure. It ensures data integrity and authenticity by digitally signing DNS records, thwarting unauthorised alterations or spoofing attempts. This authentication mechanism safeguards users from being directed to malicious websites or fooled into giving away personal information through DNS manipulation. It makes it easier for attackers to change where websites send you, which can lead to privacy breaches.

DANE: DNS-based Authentication of Named Entities offers significant security benefits by leveraging DNS records to authenticate digital certificates used in TLS connections. By binding TLS certificates to DNS domain names, DANE enhances security by eliminating reliance on traditional certificate authorities (CAs), reducing the risk of certificate-based attacks and rogue certificates. Not having DANE enabled means that when you visit secure websites (like those starting with 'https://') there's a higher risk that someone could intercept or pretend to be those websites. It's like having an extra lock on the door to make sure only the right people can come in.

HTTPS: Hypertext Transfer Protocol Secure encrypts data transmission, preventing eavesdropping and tampering, crucial for protecting sensitive information like login credentials, payment details and personal data from interception by malicious actors. When websites don't use HTTPS, any information you send to them (like passwords or credit card details) can be seen by others. It's like sending a postcard that anyone can read before it reaches its destination. There are other settings within this category that must also be configured such as HTTPS Redirect, HTTP Compression, HSTS to ensure the best protection.

Appendix 1.

Explanation of Website Configuration Settings (cont.)



TLS: Transport Layer Security (TLS) encrypts data transmitted between devices, preventing unauthorised access and ensuring confidentiality. TLS also provides authentication, verifying the identity of servers and sometimes clients, thwarting man-in-the-middle attacks and establishing trust in online interactions. Additionally, TLS safeguards data integrity, detecting and preventing tampering during transmission, crucial for protecting sensitive information like passwords, financial data and personal details. Not having TLS makes it easy for others to see passwords, financial details and personal information. It also means there's no way to be sure websites are real, which could lead to scams. Without TLS, data can be changed without you knowing.

Certificates: Web certificates, specifically SSL/TLS certificates, authenticate the identity of the website, assuring users they are connecting to the legitimate site and not an impostor. Additionally, certificates encrypt data transmitted between the user's browser and the website's server, safeguarding sensitive information from interception and tampering. Moreover, web certificates help build trust with users and improve search engine rankings, fostering a secure and reputable online presence for businesses and organisations.

Security Headers: HTTP security headers are additional response headers that enhance web security. They include X-Frame-Options, Content-Security-Policy (CSP), X-XSS-Protection, Strict-Transport-Security (HSTS), and X-Content-Type-Options. These headers mitigate various web-based attacks like clickjacking, cross-site scripting (XSS), protocol downgrade attacks, and MIME-sniffing attacks by controlling frame loading, specifying allowed content sources, enabling XSS filters, enforcing HTTPS usage and preventing MIME type sniffing, respectively. Not having these security headers means websites are more vulnerable to tricks that can lead to stolen information or unauthorised changes. It increases the risk of attackers secretly loading your website on their own and tricking users into clicking on harmful links.

RPKI: Resource Public Key Infrastructure ties internet number resources to their rightful owners using cryptographic certificates, allowing validation of route origination validation, reducing the risk of routing hijacks and route leaks. Overall, RPKI strengthens the security and integrity of internet routing. Without it, there's a higher risk of someone wrongly claiming ownership of internet routes or redirecting traffic to unauthorised destinations. This could disrupt services and compromise data security.



Appendix 2.

Process and Procedural Risks

Risk Management: Assessing how well risks related to cyber security are identified, evaluated and managed within the small business.

Observation: While many small businesses understand the significance of cybersecurity, the degree to which they adopt risk management practices can vary widely. Some prioritise and invest in cybersecurity, while others struggle due to resource allocation or a lack of perceived urgency. This project further raised the awareness of available resources and some simple steps that could be undertaken to address current risks.

Network Security: Evaluating the security measures in place to protect the small business network infrastructure from unauthorised access, breaches and other cyber threats.

Observation: Overcoming barriers such as resource constraints, technical expertise gaps and competing business priorities were major road blocks for small businesses to effectively address network security risks and protect their assets from cyber threats. While some small businesses do take steps to secure their networks, the level of protection differed significantly.

Data Protection: Assessing the strategies and technologies implemented to safeguard sensitive data from theft, unauthorised access or exposure.

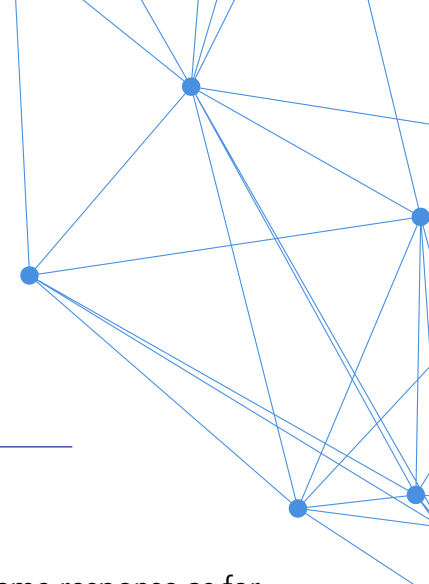
Observation: While some small businesses in Australia do take steps to protect their data, again, how much they do can really differ. Awareness of what data should be protected and what their obligations are in that respect was limited. As with some of the other areas covered by this analysis tool, the importance varied from the type of business activity and industry involved. Variations in such things as online bookings and payment systems, uploading of files to websites etc. resulted in a range of different observations on this aspect.

Endpoint Security: Evaluating the security measures applied to individual devices (such as computers, laptops, smartphones) to protect them from cyber threats.

Observation: Some small businesses do take steps to protect their devices from cyber threats, but not all do it the same way. Some rely entirely by prompts from software developers and the like. Usually if there are any significant costs involved updates are delayed, sometimes indefinitely. Some businesses avoid updates fearing they may be scams and often prefer to leave things alone due to security updates being combined with other functionality changes that are not wanted.

Appendix 2.

Process and Procedural Risks (cont.)



Incident Response: Assessing the small business preparedness and capability to respond effectively to cyber security incidents, such as data breaches or malware infections.

Observation: Where there are specifically allocated IT resources there may well be back up and disaster recovery arrangements in place, but in the main typically these processes and procedures are rarely tested for robustness within this cohort. Focus on day-to-day business activity supersedes any concerns about what ‘may’ happen in future.

Security Awareness Training: Evaluating the effectiveness of training programs aimed at raising awareness among employees about cyber security best practices and threats.

Observation: Resourcing issues and costs are the biggest impediment to employees having available time and businesses arranging effective training programs. Most employees gain their knowledge via media reports and often don’t fully understand how scams and cyber threats actually operate. With respect to specific business threats in the SMB cohort, the knowledge, if it exists, tends to be invested in individuals rather than across the employee base.

Policies and Procedures: Assessing the existence and effectiveness of policies, procedures and guidelines related to cyber security within the small business.

Observation: Much the same response as for ‘Security Awareness Training’ above. Larger businesses may have documented processes and procedures in place but varied situations regarding whether employees are aware of, or have read those documents.

Supplier and Third-Party Risk Management: Evaluating the measures in place to assess and manage cyber security risks associated with suppliers, partners and third-party vendors.

Observation: Those businesses that do not have a good security posture with respect to the other aspects covered by this analysis tool do not take any measures with respect to third party risk management. In fact we did not observe any business taking on this issue as part of their own cyber risk management strategy. The general perception was that everyone should be looking after their own status.

Legal Issues: Assessing the knowledge base of the business with respect to legal liability and related legislation such as the privacy act.

Observation: Not much knowledge and in some cases no awareness of potential legal liability or privacy issues with respect to data breaches etc. A perception that these are matters that only big businesses need to worry about, was coming through in some instances.



Appendix 3.

Thank you to the contributors of this report

A special thank you to the many individuals who contributed to developing the content of this report either directly or through the feedback provided during and after completion of the project roll out.

Sponsors & Stakeholders:

- Victorian Government Departments and Victorian Skills Authority
- Microsoft
- National Australia Bank
- Small Business Commissioner
- COSBOA
- auDA
- Business.gov.au

Business Representatives (52)

- Various Industries
- Various locations across Victoria
- Varying sizes

TAFE Personnel & Learners (138):

- Chisholm TAFE
- Kangan TAFE
- Holmesglen TAFE
- Melbourne Polytechnic
- Swinburne University
- Victoria University

Industry Mentors (16):

- Microsoft
- National Australia Bank
- Individual Industry Sources

**Findings of the 2022–2024
Victorian Government Funded Cyber Security
Risk Analysis Project**

For more information on this project, please contact:

Dominic Schipano
dominics@citt.com.au



CITT

Providing Strategic ICT Advice within the Australian
Digital and Telecommunications Industry