Cyber Security Market in Sunshine Coast in Australia

Table of Contents (TOC)
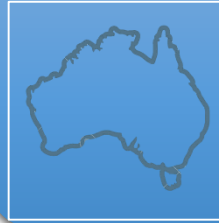
Chapter: 1

Executive Summary

Executive Summary

Market size of Cyber security market in Australia is estimated to be USD 3.7 Billion in 2019. Expected to grow at 10.81% during 2020-25.

Market size of Cyber security market in , Sunshine Coast is estimated to be USD 215 Million in 2019. Expected to grow at 11.68% during 2020-25.

Small & Medium size business are potential market to target which is expected to grow at CAGR of 12.89% during 2020-25 to reach USD 189 million.

BFSI, Healthcare, IT & Telecom are some of the potential industries which are expected to grow in terms of market opportunity for Cyber security market in Sunshine Coast.o reach USD 189 million.

Chapter: 2

Market Overview

Cyber Security Market Overview

- The global cyber security market is booming the market has grown more than 30x in last 13 years.

- The U.S. 2019 President's Budget was $15 billion for cyber security-related activities, and France has committed to 4,000 cyber headcount by 2025.

- Every year 300+ new startups launching and VCs investment in cyber security was a record high of USD 5.3 billion in 2018 & more than USD 6 billion in 2019.

- As per a recent report by Gartner Group, organizations are increasingly investing in cyber security, showing security spending is outpacing IT spending. Security departments are expanding in size and budget, and, at the helm, security decision-makers are gaining respect more than ever before. With ever-dynamic cyber security risks and regulations, it is clear to most C-suite leaders that there's more to be protected and more on the line.

- Security is taking on a new shape within organizations. Generally, security buyers are investing in various categories in order to protect their organizations. Moreover, security is often integrated into new business initiatives and used as a competitive advantage.

- New categories emerge in spaces like Zero Trust and IoT security to address threats that are growing in scope and sophistication.

Cyber Security Market Overview

- **Impact of rising awareness among Customer :** High magnitude attacks geared toward B2C companies could lead to massive customer churn and bottom-line damage. The awareness level of consumers to cyber security and privacy is already raising the bar for companies to beef up their security efforts. As a result of higher customer expectations and intensified regulation, many companies will further invest in security and the market will keep expanding, respectively.

- **Impact of Economy :** In its Global Risk Report 2018, the World Economic Forum (WEF) listed cyber threat as one of the most critical risks threatening the world economy. In the near-term, companies will likely incur paralyzing attacks that will shut down daily operations, causing unprecedented loss of revenue eclipsing. These crippling cyber attacks will lead to direct growth in cyber security spend.

- **Impact on Civil-life :** Attacks on developed countries could interrupt electricity, water supply and more, causing massive civil-life disorder. In addition, the rise of IoT and autonomous machinery in our day-to-day will not only expand the attack surface, but also threaten lives. The safety of people will pressure political bodies into creating regulatory requirements to bolster security for embedded technologies and scrutinizing how smart devices are secured.

- AU$2.3 billion was stolen by cyber criminals from Australian consumers in 2017; while 53,474 reports were received by the Australian Cybercrime Online Reporting Network (ACORN) in the 2017-18 financial year, and another 64,528 in 2018-19. 964 data breach notifications were also made under the Notifiable Data Breaches scheme from April 2018 to March 2019, 60% of which were malicious or criminal attacks.

- One big attack was recently held on the Australian Parliament when some foreign state-sponsored hackers breached the Australian parliament's computer systems. However, Australian defensive agencies detected it and confronted this attack. This attack revealed the need for investment in cyber security in Australia.

- Another attack on Australian National University where the university was under cyber attack and the cyber hackers gained the information of about 200,000 students and staff. It was the 2nd big attack on the university in just a year, it raised concerns that foreign forces are trying hard to capture delicate information about students and may miss use it in the future.

- With the second-highest 'cyber maturity' in the Indo-Pacific region and strengths in core skill areas such as quantum computation, wireless technology and high-value niche hardware, Australia is the ideal growth environment for cyber security businesses.

Cyber Security Market Overview - Australia

- Every year in Australia, there are thousands of data breaches and malware attacks to organizations, research institutes, and businesses. Most of these breaches affect small businesses; occasionally there are major cyber breaches that have impacted larger organizations and a huge amount of people.

- There is a growing trends of homegrown cyber security firms catering to specialty in fintech, which is a move that is part of a government and industry effort to be less dependent on technologies from overseas to secure the country's infrastructure.

- The Cyber Security Growth Centre, which will receive AU$30 million in federal funding through 2020, will coordinate the effort. Last December, the government launched the Australian Cyber Security Growth Network, a not-for-profit company to oversee the rollout. A Cyber Security Innovation Lab will be created to help commercialize cyber security innovation in fintech, working with researchers, companies and government agencies.

- Australian cyber security sector is small, but quickly growing in maturity and size, with an increasing number of home-grown success stories. Australian cyber security software, hardware and services companies have joined global value chains and are establishing a worldwide reputation for high quality, deep tech, niche solutions for increasingly complex cyber risks in a highly contextual, hostile cyber-physical environment.
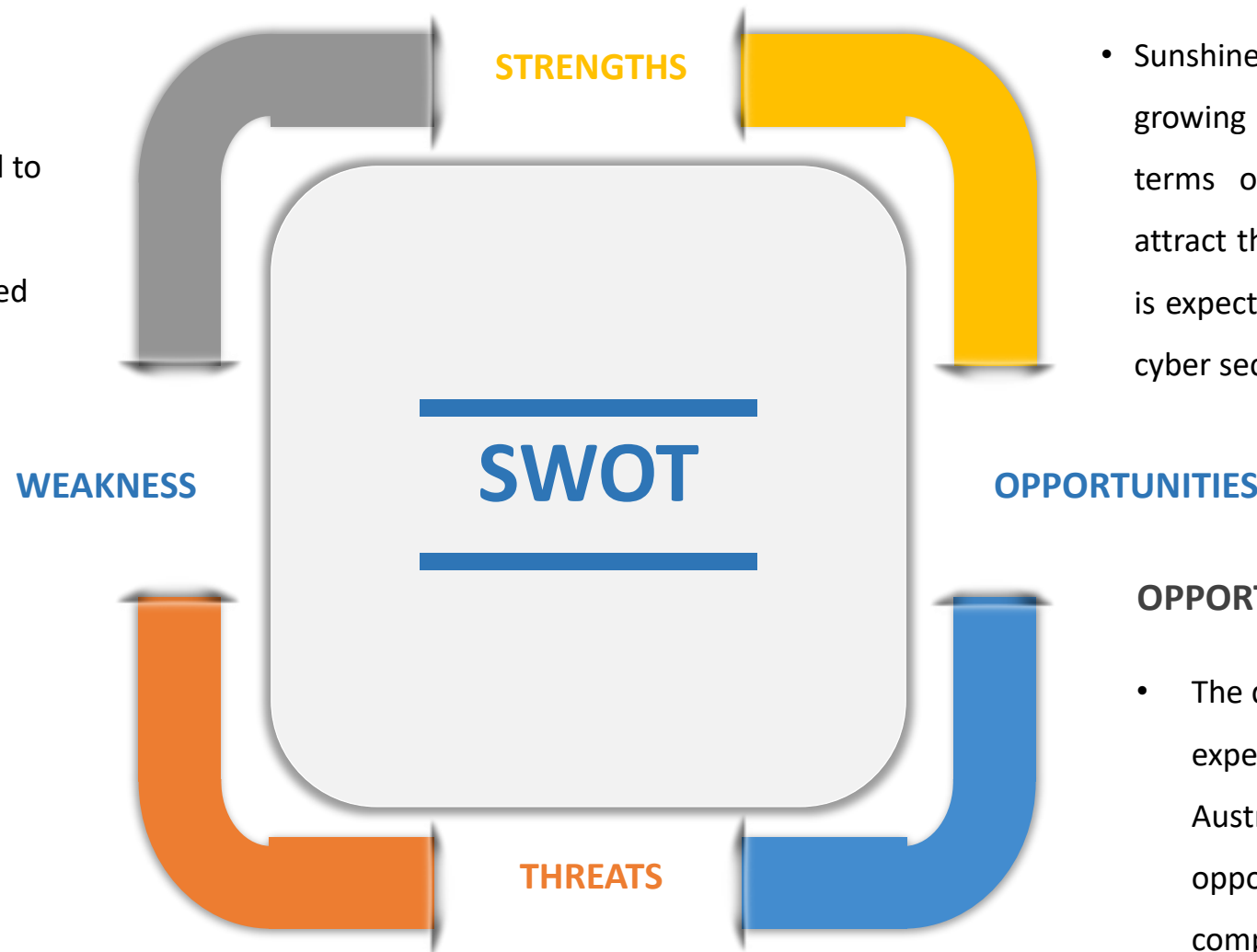
SWOT Analysis

WEAKNESS

- Most of the companies are providing multi-service related to IT, Network. No company is providing cyber security focused service.

THREATS

- Lot of foreign player are also entering into Australian market which become threat to local players in Sunshine coast later.

STRENGTH

- Sunshine coast being the most growing & 9th largest government in terms of economy is expected to attract the attention of hackers which is expected to raise demand of strong cyber security network.

OPPORTUNITIES

- The demand for cyber security is expected to raise in all over Australia which would open up opportunity for solution provider companies based in Sunshine coast .

STRENGTHS

WEAKNESS

SWOT

OPPORTUNITIES

THREATS

10

Porter's 5 Forces
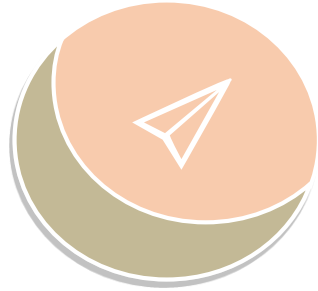
Threat of new entrants

Threat of substitutes

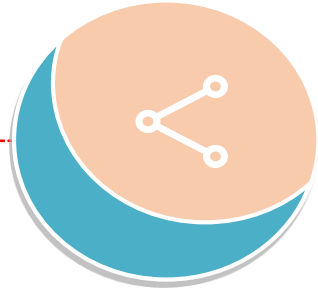**Bargaining power of customers**

Bargaining power of suppliers

Competitive rivalry

- There are less entry barrier for new entrants in Australia if they have proper certification. Established player can easily enter into the market & can become threat for local players.

- There are no such threat of substitution of cyber security.

- Australia cyber security market is competitive specially in Sunshine coast area where there are many players. Due to competition bargaining power of customers are high.

- Bargaining power of companies is comparatively low. All players try to maintain price as competitive as they can.
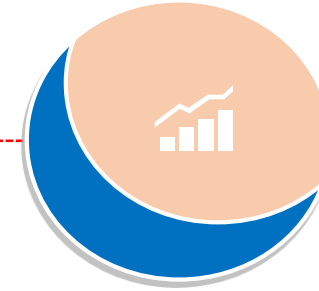
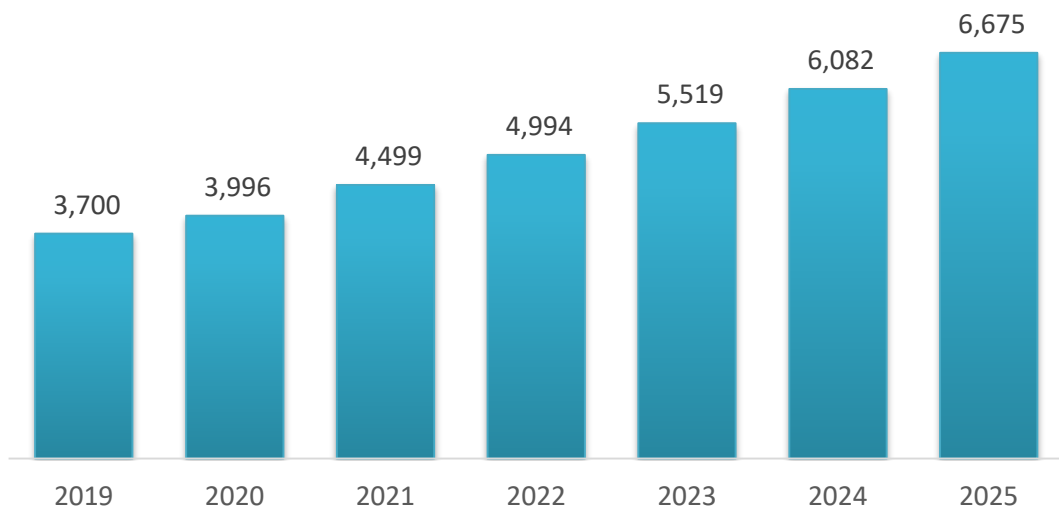- Competition is high Sunshine coast area in Australia since there are many players in the market.
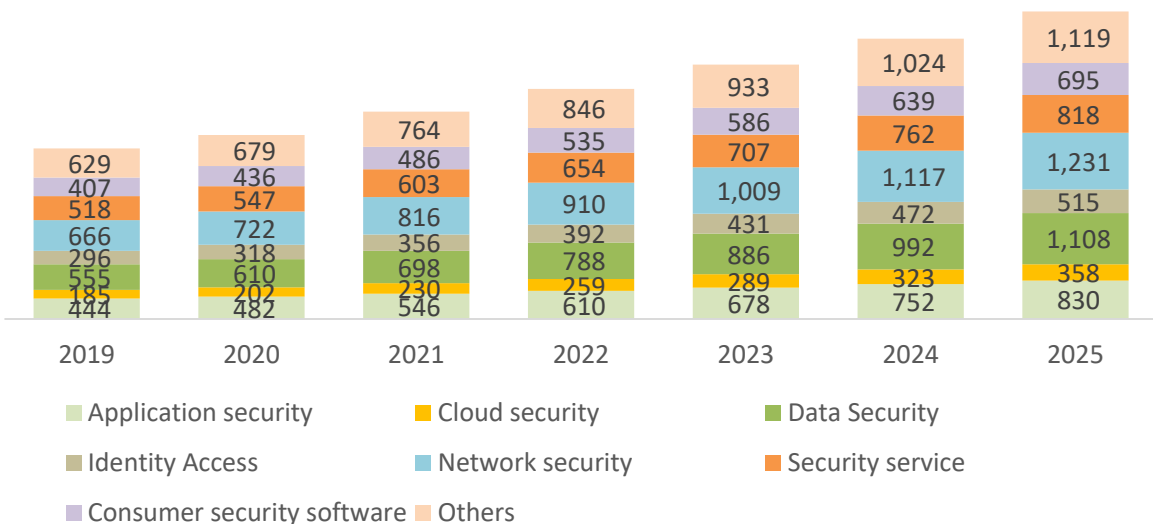
Chapter: 3

Market size estimation

Cyber Security Market Size - Australia

MARKET SIZE (USD MILLION)

Bar chart values:
- 2019: 3,700
- 2020: 3,996
- 2021: 4,499
- 2022: 4,994
- 2023: 5,519
- 2024: 6,082
- 2025: 6,675

- Market size of Australia Cyber security is estimated to be USD 3.7 billion in 2019. The growth of the market would be slightly hamper in 2021 due to lower budget allocation due to current economic & pandemic crisis but there would be still some growth in 2020 since more company would adopt work of home & need of cyber security would be need of the hour which would be a new trends from 2020.

MARKET SIZE BY TYPE(USD MILLION)

Type	2019	2020	2021	2022	2023	2024	2025
Others	629	679	764	846	933	1,024	1,119
Consumer security software	407	436	486	535	586	639	695
Security service	518	547	603	654	707	762	818
Network security	666	722	816	910	1,009	1,117	1,231
Identity Access	296	318	356	392	431	472	515
Data Security	555	610	698	788	886	992	1,108
Cloud security	185	202	230	259	289	323	358
Application security	444	482	546	610	678	752	830

Legend:
- Application security
- Cloud security
- Data Security
- Identity Access
- Network security
- Security service
- Consumer security software
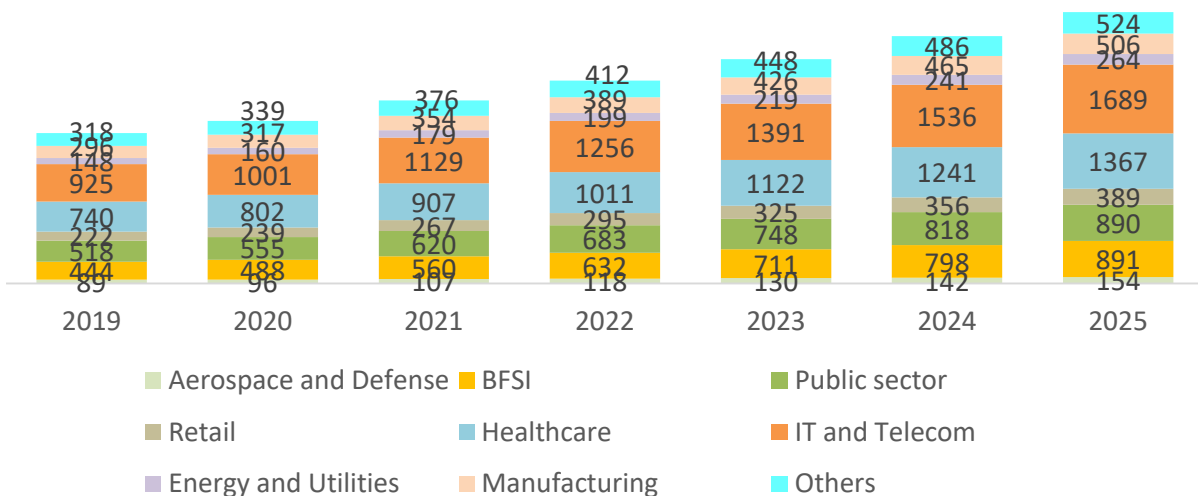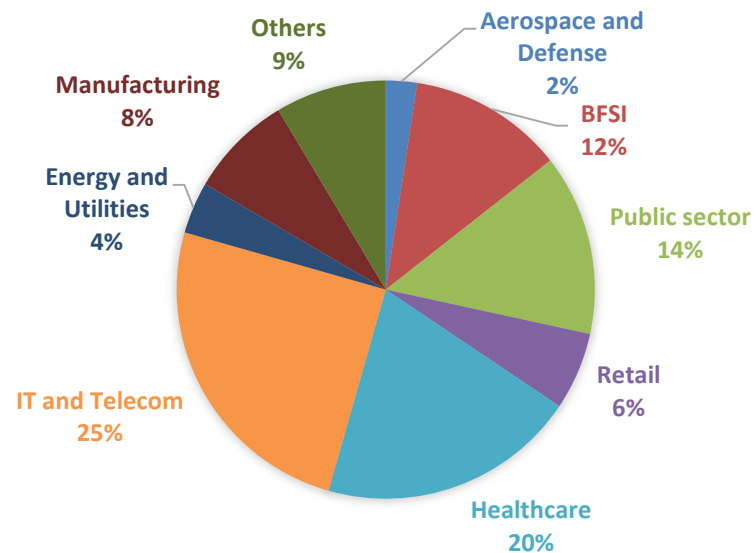- Others

- Network security, Application security, Data security, Consumer security software, security services are of the prominent type in terms of market size.
- Cloud security, Data security are the two most prominent type in terms of future market growth during 2020-25.
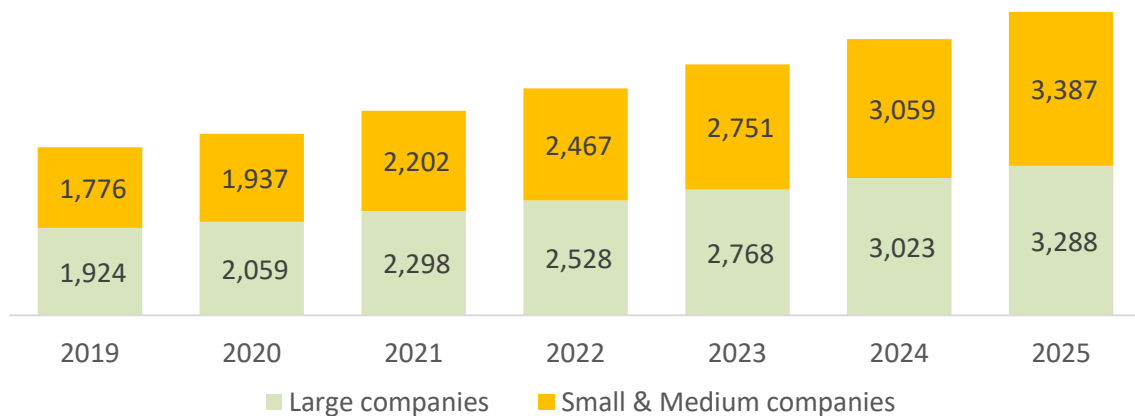
13

Cyber Security Market Size - Australia

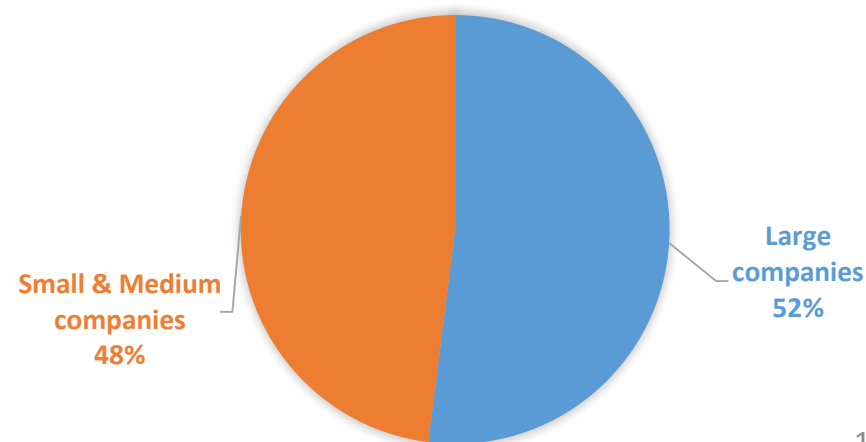## MARKET SIZE BY CUSTOMER APPLICATION INDUSTRY (USD MILLION)

Year	Aerospace and Defense	BFSI	Public sector	Retail	Healthcare	IT and Telecom	Energy and Utilities	Manufacturing	Others
2019	89	444	518	222	740	925	148	296	318
2020	96	488	555	239	802	1001	160	317	339
2021	107	560	620	267	907	1129	179	354	376
2022	118	632	683	295	1011	1256	199	389	412
2023	130	711	748	325	1122	1391	219	426	448
2024	142	798	818	356	1241	1536	241	465	486
2025	154	891	890	389	1367	1689	264	506	524

Legend: Aerospace and Defense, BFSI, Public sector, Retail, Healthcare, IT and Telecom, Energy and Utilities, Manufacturing, Others

BY INDUSTRY APPLICATION - 2019

- Others 9%
- Aerospace and Defense 2%
- BFSI 12%
- Public sector 14%
- Retail 6%
- Healthcare 20%
- IT and Telecom 25%
- Energy and Utilities 4%
- Manufacturing 8%

BY CUSTOMER COMPANY TYPE (USD MILLION)

Year	Large companies	Small & Medium companies
2019	1,924	1,776
2020	2,059	1,937
2021	2,298	2,202
2022	2,528	2,467
2023	2,768	2,751
2024	3,023	3,059
2025	3,288	3,387

BY COMPANY TYPE - 2019

- Large companies 52%
- Small & Medium companies 48%

14

Cyber Security Market Size – Sunshine Coast

MARKET SIZE (USD MILLION)

402

37

36

33

32

32

17

215

2019 2020 2021 2022 2023 2024 2025

■ New Opportunity
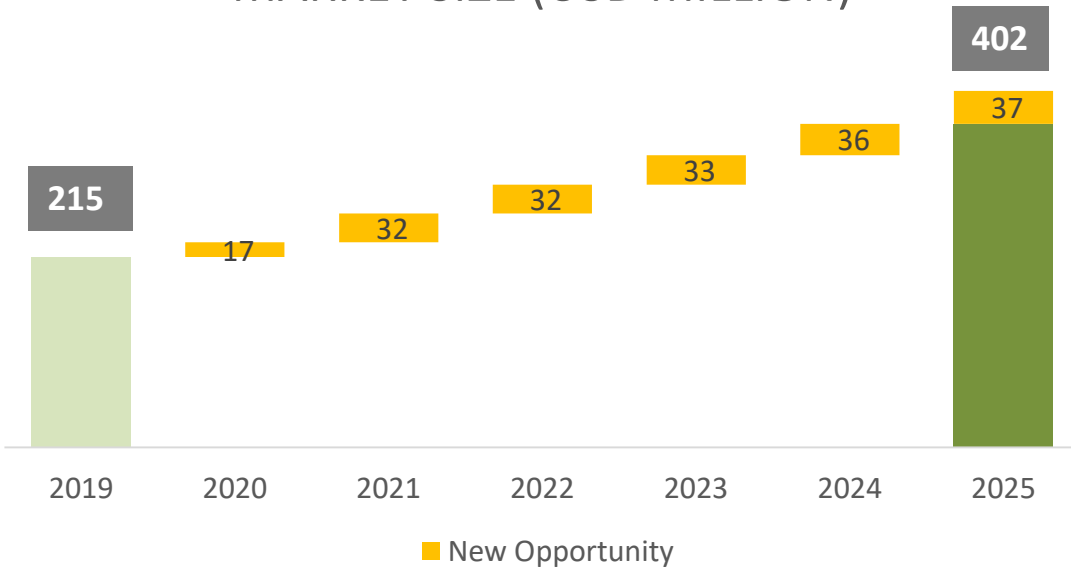
- Market size of Cyber security in sunshine coast Australia is estimated to be USD 215 million in 2019. The market is forecasted to grow to USD 402 million by 2025 at a CAGR of 11.68% during forecasting period of 2020-25.
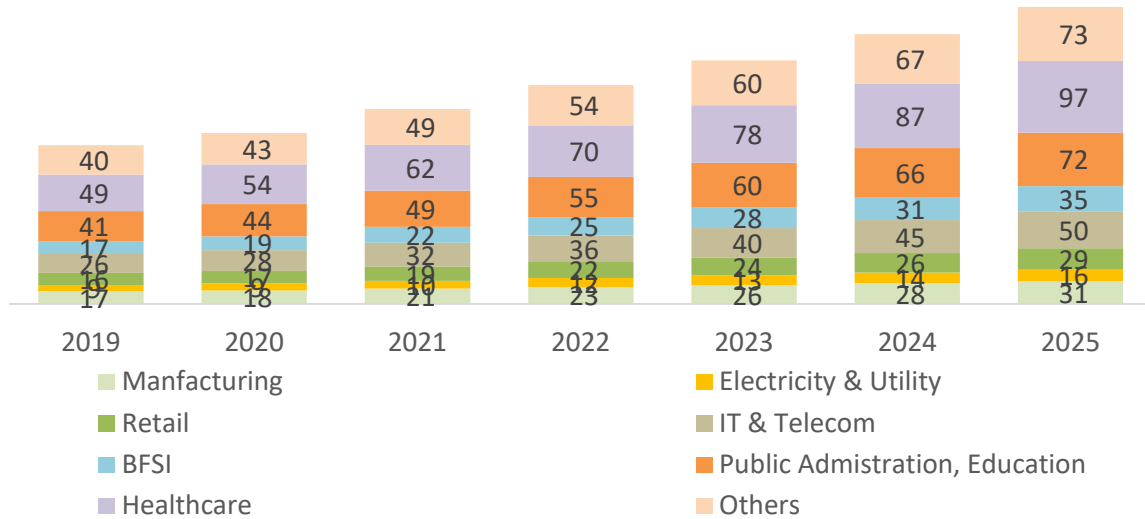
MARKET SIZE BY TYPE (USD MILLION)

	2019	2020	2021	2022	2023	2024	2025
Others	17	18	20	22	24	26	28
Consumer security software	36	39	44	49	53	58	64
Security service	26	27	31	34	38	41	45
Network security	43	47	54	61	69	77	85
Identity Access	24	25	29	32	36	40	44
Data Security	45	49	57	64	72	81	90
Cloud security	9	9	11	12	14	16	18
Application security	15	16	19	21	23	26	28

■ Application security   ■ Cloud security   ■ Data Security
■ Identity Access   ■ Network security   ■ Security service
■ Consumer security software   ■ Others

- In Sunshine coast network security, consumer security software, data security, security service are some of the potential market to focus on.
- Cloud security & data security are some potential area in terms of growth in future.

15

MARKET SIZE BY CUSTOMER APPLICATION INDUSTRY (USD MILLION)

Legend:
- Manfacturing
- Retail
- BFSI
- Healthcare
- Electricity & Utility
- IT & Telecom
- Public Admistration, Education
- Others

- In terms of application industry Healthcare, Public administration, IT & Telecom are the largest user of cyber security service in Sunshine coast.
- BFSI, IT & Telecom, Healthcare Industry are also expected to higher budget from client in future for cyber security.

MARKET SIZE BY COMPANY TYPE (USD MILLION)

Legend:
- Large companies
- Small & Medium companies
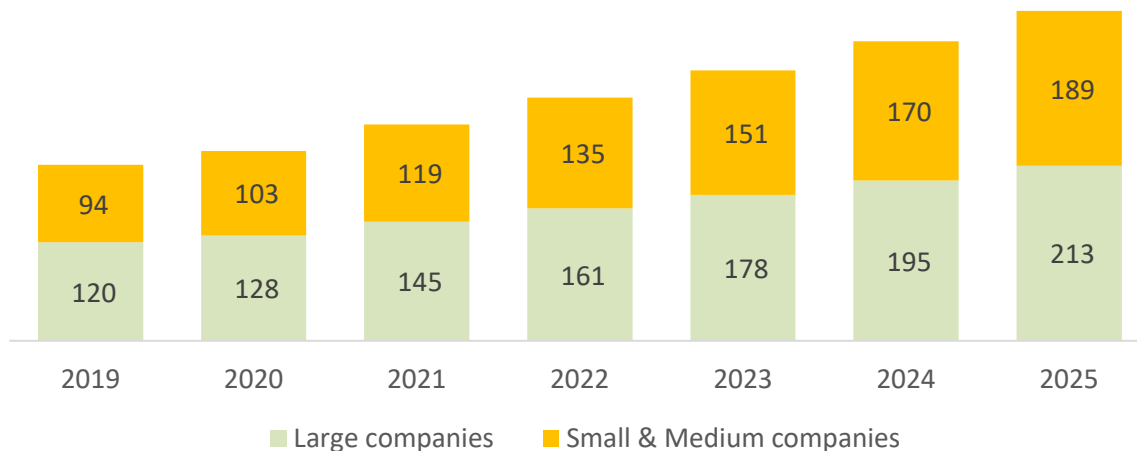
- In Sunshine coast area Large companies are major user of cyber security at present.
- In future use of cyber security in small & medium companies are expected to grow much faster than larger companies.
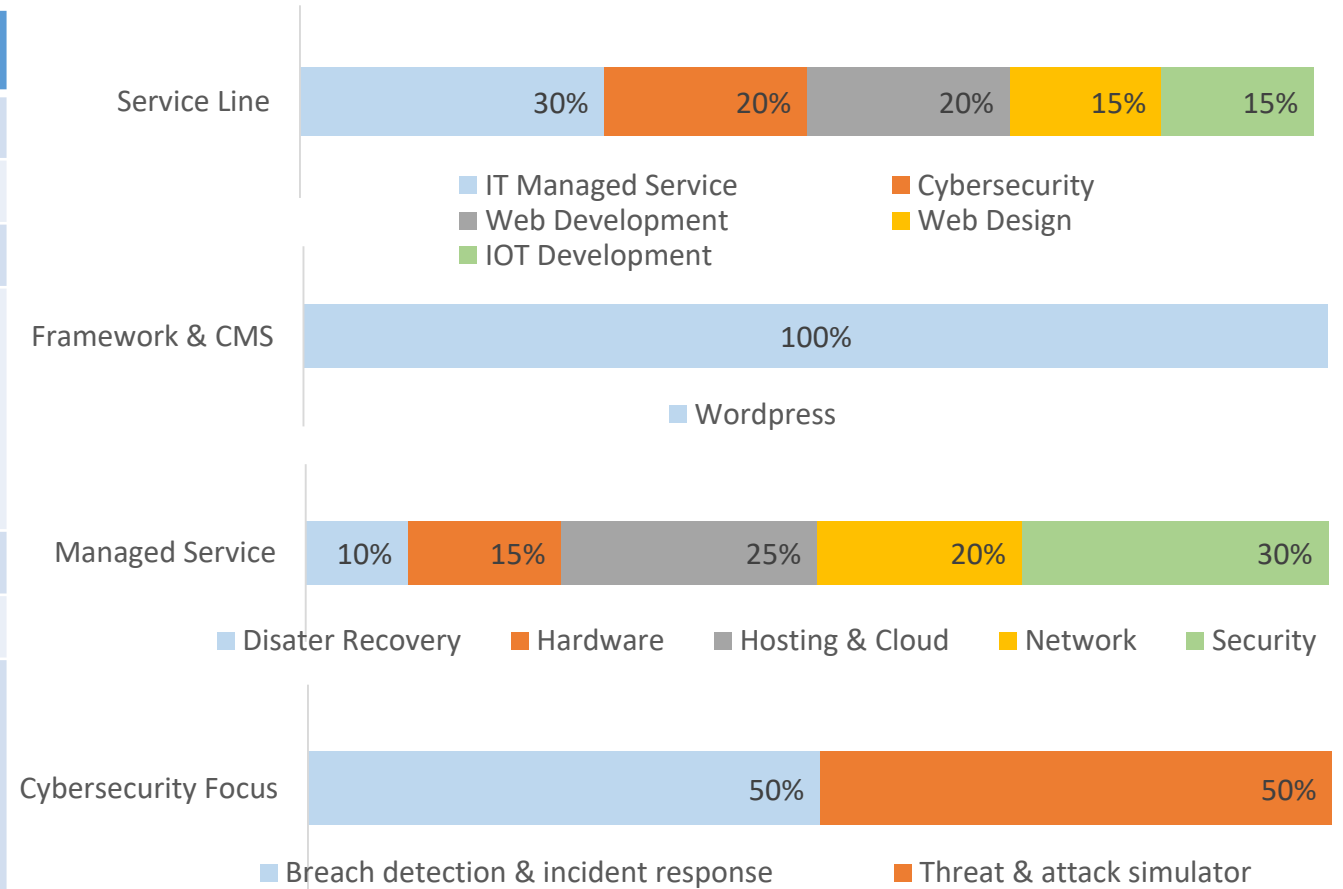
16

Chapter: 4

Competitors Analysis

Competitors Analysis

Company Name	Prosnet Business IT
Type	Private
Founded	2008
Headquarter	Maroochydore, Australia
Focus Area	Provide services in also Brisbane, Sunshine Coast, Gold Coast, Maryborough, Gympie, Bundaberg, Hervey Bay and Byron Bay.
Revenue	N/A
Number of employee	Below 10
Services Provided	• Managed IT service • Network Solutions • Cloud Solutions • Microsoft Office 365 • IT Security • Data Analysis • Software Web Development • IOT
Website	https://prosnet.com.au/

Service Line

30%	20%	20%	15%	15%

- IT Managed Service
- Cybersecurity
- Web Development
- Web Design
- IOT Development

Framework & CMS

100%

- Wordpress

Managed Service

10%	15%	25%	20%	30%

- Disater Recovery
- Hardware
- Hosting & Cloud
- Network
- Security

Cybersecurity Focus

50%	50%

- Breach detection & incident response
- Threat & attack simulator

IT & Network Security Service

It provides IT Disaster Recovery (Mainly UPS), Internet Security, Firewalls.

Industries Served:- *Retail & Wholesale, Education & Human Resources, Accounting & law Firm, Construction & Engineering, Medical & Real Estate*

Strength

- Various service offering which attracts larger demands across various industries.
- On-site and Remote Support, Emergency Support Service for all clients
- IT Disaster Recovery Plan to ensure business continuity and elasticity.

S

W

Weakness

- Prosnet has very less expertise in Cyber security service.

Competitors Analysis

Company Name	Computer Networks at Ease
Type	Private
Founded	1995
Headquarter	Warana, Australia
Focus Area	Provide services Pan-Australia. Have presence in Fiji also.
Key People	Ralph Kowalczyk, Founder
Revenue	USD 3.2 million
Number of employee	12
Services Provided	• Networking & Monitoring • Sage Consulting & Implementations • Broadband Services • Document Management
Website	https://cnae.com.au/

Service Line

20%	20%	35%	15%	10%

- Networking & Monitoring
- Consulting & Implementation
- Broadband Services
- Document Management
- Cybersecurity
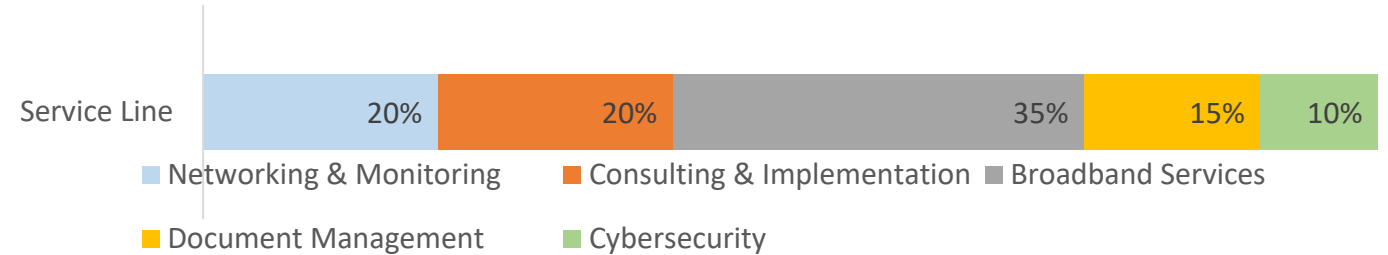
Security

CNAE offer Antivirus, mail washing and filtering, WAN solutions, VPN and Firewall solutions to its customers. CNAE also provide systems, monitoring, and reporting so that customer are kept up to date and informed about what's going on in network.

Key Partners

Competitors Analysis

Strength

- CNAE has over 20 years' experience in the information technology industry.
- Variety of remote support and access methods to resolve customer service request
- Multi-layered services such as onsite, offsite, and multi-tiered backup and Disaster Recovery solutions.

S

W

Weakness

- More focused on providing IT infrastructure service, very less expertise in Cyber security service.
- Very less active in social media pages like Facebook, LinkedIn

Competitors Analysis

Company Name	Mullins IT
Type	Private
Founded	2000
Headquarter	Parrearra, Queensland, Australia
Focus Area	Provide services in Sunshine Coast, Brisbane and Central Queensland Coast regions.
Key People	N/A
Revenue	USD 600K
Number of employee	3-5
Services Provided	• Cloud Migration & Integration • Computer repair • Data Cabling • Disaster recovery • IT Security • Managed Services • Network Management • Network Audits & education • POS • Server management • Business & Home network solution
Website	www.mullinsit.com

Service Line

30%	20%	10%	10%	30%
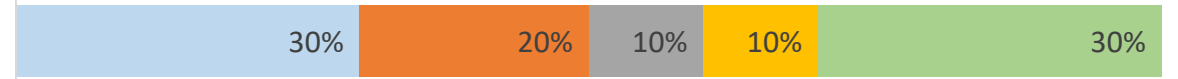
■ Cybersecurity ■ #REF! ■ Home Network Solutions ■ Business Network Solutions ■ Others

IT Security Service
➢ Anti-Malware
➢ Anti-Spyware
➢ Rootkit scanning
➢ Dedicated Firewall
➢ Content Filtering
➢ Key Logging Software Scans

Disaster Recovery Service
➢ Data Recovery Plan – Design & Implementation
➢ Data Breach Plan – Design & Implementation
➢ Business-Critical Onsite Backups
➢ Business-Critical Cloud Backups
➢ Ransomware Recovery

Competitors Analysis

Strength

- Has offerings of various range of cyber security strategies and products that prevents unauthorized access to critical assets such as computers, networks, and data.
- It maintains the integrity and confidentiality of sensitive information, blocking the access of sophisticated hackers.
- Its Disaster recovery focuses supporting critical business functions to minimize the disruption in the event of a significant disruptive event such as a data breach or ransom ware attack occurring.
- Very Active on Social Media such as Facebook.
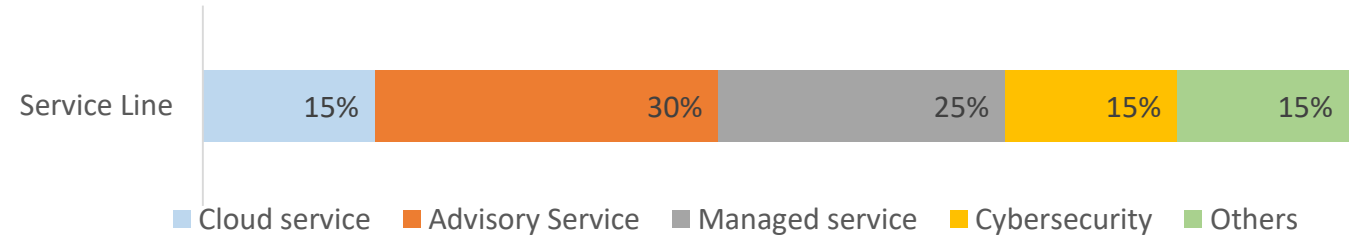
S

W

Weakness

- No good portfolio build-up or case study in the website to showcase to the client except a few customer review.
- Not active in professional network such as LinkedIn

Competitors Analysis

Company Name	Secure Access
Type	Private
Founded	1999
Headquarter	Maroochydore, Queensland, Australia
Focus Area	Focussed on South East Queensland .
Key People	Jason, Founder & CEO
Revenue	USD 6 million
Number of employee	35
Services Provided	• Cloud Services • Technology Advisory Services • Managed Services • Project & Technical Services • Communication & Connectivity • Security Services
Website	www.secureaccess.com.au

In 2015 Secure Access received a CRN Fast 50 award, which recognizes the fastest growing technology businesses in Australia.

Service Line

15%	30%	25%	15%	15%

■ Cloud service ■ Advisory Service ■ Managed service ■ Cybersecurity ■ Others

Security Service
➢ Anti-Virus
➢ Endpoint Protection
➢ Email filtering
➢ Internal and external security assessment services
  • Vulnerability scanning
  • Exchange
  • SQL
  • User and file audits
  • PCI compliance assessment

Key Partner

D-Link — Building Networks for People

hp

CyberPower — Reliability. Quality. Value.

vmware

Microsoft Partner — Gold Midmarket Solution Provider / Gold Small and Midmarket Cloud Solutions — Microsoft

intel

cisco

Competitors Analysis

Strength

- Secure Access strategy involves more customer centric approach like alignment of customer's technology plan with customer business strategy.
- Active in Social & Business Media Platform like Facebook, LinkedIn, Twitter
- Well Experienced Team having certifications from Microsoft, VMware, Dlink, Xirrus, Sonicwall, Google, Apple, Nible storage

S

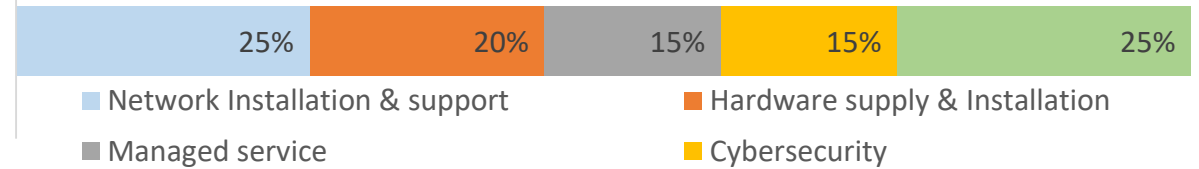**W**

Weakness

- More focused on local East Queensland business. Business in Pan-Australia & International market is less.

Competitors Analysis

Company Name	CRT Network Solutions
Type	Private
Founded	2006
Headquarter	Maroochydore, Queensland, Australia
Focus Area	Brisbane and the Sunshine coast
Key People	Chris, Director
Revenue	USD 31 million
Number of employee	165
Services Provided	• Server & Network Installation • Network IT Support • Hardware supply & installation • Managed IT Service • Website design • Disaster Recovery Plan • Medical IT Support
Website	www.crtnetworksolutions.com.au

Main Focussed Industries:- *Medical Software companies followed by Architectural and legal firms , chiropractic offices and large fencing companies.*

Service Line	25%	20%	15%	15%	25%

- Network Installation & support
- Hardware supply & Installation
- Managed service
- Cybersecurity

Security
Data Integrity, Server Monitoring, CRT Firewall, Antivirus

Disaster Recovery Plan
➢ File and Data Loss
➢ Power Outage
➢ Human Error
➢ Full loss of site and system in the event of a major event such as a flood
➢ Equipment Theft
➢ Faulty Hardware
➢ Loss of key staff members

Key Customers

Big medical software companies such as:-

o Best Practice
o Medical Director
o Pracsoft

o Blue Chip
o Zedmed
o Genie Medical

o Practix
o RX & many other software companies

Competitors Analysis

Key Partner

Strength

- Strongly Focused on Medical IT market which is a growing market.
- Various service offering catering to each & every industries in the local market
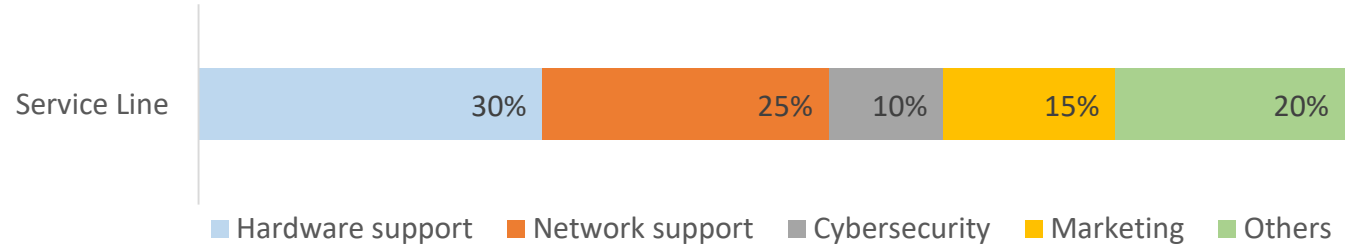
S

W

Weakness

- Very less social media presence.
- Less exposure in International business

Competitors Analysis

| Company Name	Absolute I.T.
Type	Private
Founded	2006
Headquarter	Maroochydore, Queensland, Australia
Focus Area	Greater Sunshine Coast region from Caloundra up to Noosa & Tewantin
Key People	Trent Nuske, Co-Owner
Revenue	N/A
Number of employee	10-15
Services Provided	• Remote work • Video Conferencing • Apple, Windows, Linux device repair & support • Data Backup & recovery • Internet & network solution • Website, SEO, Social media • Computer set-up, repair, Printer • IT Solution • Anti-virus solution
Website	https://www.absolute-it.com.au/

Service Line

30%	25%	10%	15%	20%

■ Hardware support   ■ Network support   ■ Cybersecurity   ■ Marketing   ■ Others

Security service
➢ Backups of all important data to off-site server
➢ Anti-virus solution
➢ Networking hardware installed to stop viruses
➢ Monitoring & managing Firewall settings

Data backup and recovery solutions
➢ Offsite backups to their repository
➢ Regular check of backups progress with data recovery checks

Key Partner
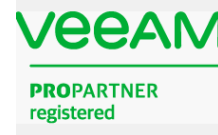
Strength

- Besides cyber securiy provides other related service such as Website security, consultation on Physical security such as alarms, cameras, locked doors, computer lockdown cables, etc.
- Have certified IT specialist from Kounta, Veeam, Microsoft, Cisco

S

W

Weakness

- Have presence in all social media platform but not active except Instagram where it focuses on its video marketing service.

Competitors Analysis

Company Name	Directions Technology
Type	Private
Founded	1993
Headquarter	Brisbane, Queensland, Australia
Focus Area	Brisbane, CBD, Milton, Acacia Ridge, and Murarrie
Key People	Lachlan McIntosh, CEO
Revenue	USD 4 million
Number of employee	30+
Services Provided	• Managed IT service • IT Project delivery • Cloud Computing service • IT product sales • Custom software development
Website	https://www.directionstech.com.au/

Service Line

25%	20%	25%	10%	20%

- ■ Managed IT service
- ■ Cloud Computing
- ■ Custom Software development
- ■ Cybersecurity
- ■ Others
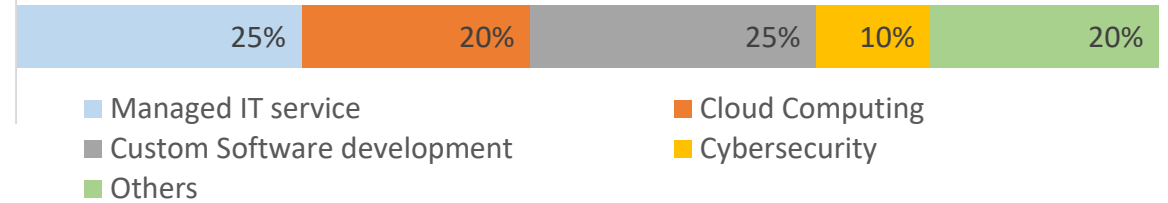
Security & Data Back-up services
- ➢ Managed Firewall
- ➢ Managed Remote Back-up
- ➢ Network Security Solutions
- ➢ Enterprise Storage and Backup Implementation
- ➢ Secure Remote Access

Key Partner

Competitors Analysis

Strength

- Focused on providing service to small business in Sunshine Coast region
- Strong capability in managed IT services & software development
- 24X7 service available to client
- Engaged in marketing activities through referral programs which surely helps it to get more clients

S

W

Weakness

- Less presence in cyber security services
- Very less social media presence

Marketing Strategies

Create awareness amongst the potential customers

Your potential customer must be aware of the cyber security issues and risk of data breaches for their business. Different survey shows that the lack of awareness and support among the executives have made significant challenges in developing effective marketing strategies. You should focus on developing content marketing with the coordination of cyber security experts & content writer which would help them to build credibility while addressing the unaware client.

Research on potential customer & Industry

Focus on certain industries & try to find-out potential customers who have not started or using cyber security service at minimal stage. Reach out to those customer through targeted email or LinkedIn to showcase how their company are vulnerable to cyber attacks & also show how your product can protect from such potential threat. Ask for a demo of your product which would help your potential clients to have a look & feel of your product live & easier to convince them to subscribe your service.

Maintain Credibility and Trustworthiness

In order to meet the credibility of the cyber security business, you should offer their potential customers with specific and unique solutions to meet their requirements because the customers don't look for a good solution to expand and improve their business but they also look for a unique solution to protect their business from cyber threats.

33

Increase Your Testimonials

Nothing speaks to the credibility, reliability, and trustworthiness of your brand and cyber security company quite like a customer testimonial. When signing the client on and during the pricing phases, offer a chance for a better price if they are willing to provide a written or video testimony about their experience with you. This still gives the consumer control over their feedback, and you have a great resource to both learn from and use as proof of your product's value. This is an extremely powerful method as it allows you to construct case studies to show potential customers how your brand analyzed a security problem, provided a valuable solution (your service), and eased them through the entire process.

Create Credible Content

In the cyber security sector, your audience will want to know top techniques or best practices. They also enjoy hands-on approaches like, "How to execute xyz on your network" or "6 Tips to Securing Your Data." This type of content usually provides step-by-step instructions and is considered evergreen content - content that is reusable and not just related to current events so you can use it to generate leads or even as a sales asset long after it's initially written. Providing your customers with content that advises them and gives them real value will create new doors for prospects to ask more questions while evaluating your service or product.

Marketing with social media

One of the most important marketing steps you can take today is to engage in social media. You need to have a variety of social media accounts, from Facebook to Twitter. Make sure that you're updating these account regularly. If you have the account but no information or posts, people aren't going to "Like" your page or follow you as a friend.

There are many different types of updates you can have on your social media accounts. Consider linking to relevant and interesting news articles. This will help get people talking about your company and what you do. In addition, consider adding safety tips to your social media account. As a cyber security company, you should stress the importance of identity theft protection when people are using social media.

Pay Per Click Advertising

Many cyber security companies find that pay-per-click advertising is a great way to go. This option allows you to get at the top results of the search engines. You have to pay for the advertising, but depending on the keywords you're targeting, it can be cheap or extremely expensive. You need to look at your competition and the PPC prices. It's a good idea to research a number of keyword options to ensure that you're not going over budget on your marketing.

The great thing about PPC marketing is that you can set it up and find out what is working for your company and what isn't. You can make changes to your advertisements to ensure that you're getting the most for your money.

35

Create an Email Marketing Campaign

There are several ways you can go about creating and maintaining an email marketing campaign. These campaigns are effective because more people are getting their emails straight to their phones. This means that they're more likely to get your email and look at it.

There are a few different ways you can get emails for your campaign. You can purchase an email list. This will cost you money, but it'll give you a great starting point. Another option is to create your own list. One of the best ways to do this is to offer something in return for an email address. An e-book about security and personal safety is a great option.

Send Out Mailers

Age old Mail marketing is still an important part of your marketing strategy. When you're creating a mailer, make sure that it is compelling and that it draws in the customer. One good way to go about this is to offer potential customers coupons and other great offers through the mailer.

Thank You