TMS

STATE OF THE NATION SERIES

Delivered to You by:

FUJITSU

ICT in Thailand

Report 4: Cybersecurity

STATE OF THE NATION

About the TMS State of the Nation: ICT in Thailand Report

Real Insights from Real ICT and Business Decision Makers

We recognize that business leaders, especially those responsible for ICT decision making have a difficult job. Budgets are tight, and management demands more accountability and greater ROI from their ICT investments. In addition, ICT professionals need to maintain and improve the current mission critical systems, whilst simultaneously driving Digital Transformation to compete in the market.

Read the Views of ICT Decision Makers in Thailand

To shed light on these challenges we went to the ICT Decision Makers themselves – people like you who can provide real insights grounded in real experience. Technology & Management Services (TMS) an ICT research and advisory firm with a specific focus on Asia/Pacific, surveyed ICT decision makers in Thailand.

After fielding surveys to over 10,000 potential respondents, TMS were able to collect high quality, valid completed responses from 107 ICT Decision makers in Thailand

Balancing Existing Systems and Advancing DX

Unlike many other recent ICT reports about the *digital economy and digital transformation*, this report also paints a comprehensive picture of the relative strengths and weaknesses of the *current state of ICT implementation and investment* in Thailand.

This is important for ICT decision making as the majority of ICT budgets are spent on '*keeping the lights on'* and maintaining and upgrading existing infrastructure and applications.

ICT Decision Makers Need Clarity

However, the need for *Digital Transformation* is increasing, and ICT decision makers often don't have time to cut through multiple, confusing, conflicting and biased sources of advice. Importantly, to provide some clarity, this report series provides detailed analyses of the ICT Decision Makers' *Business Strategies and associated ICT Strategies; Staffing and Budget intentions and Sourcing considerations*.

DX Drivers, Challenges and Investment Plans

In addition, the report series covers, *Digital Transformation Drivers, Challenges; and Implementation and Investment directions* for a range of digital transformation technologies or strategies including: *AI, IOT, Cloud, Cybersecurity, Workplace Innovation, Enterprise Applications*, and related topics.

A Unique Report

We believe this to be the first survey of this scope and size conducted in Thailand. Almost every aspect of current and future ICT plans and issues have been covered. Many questions are related, cross-referenced, and compared. Taken in their totality they build a comprehensive picture of the issues and challenges facing ICT Decision makers in Thailand now and for the next 12 to 18 months.

TMS DX Technology Matrix and Methodology

Complete details of the TMS Digital Transformation Technology Matrix (DXTM) which was used as the framework for development of this research, and the research method and approach are contained at the end of the report.

Foreword

Welcome to the 'TMS State of The Nation: ICT in Thailand 2019' report Series!

This is the fourth report in the series, and focuses on Cybersecurity, Business Continuity and related technologies and this important aspect of the market through the eyes of the people who actually manage and deliver these technologies – the ICT decision makers.

Cybersecurity

Governments at every level are delivering their services digitally and are opening up government data to third parties to help them develop new information-based services.

Electronic identity management has become commonplace. These changes are revolutionary. But they are not without cost. New technologies mean new opportunities, bad as well as well as good.

In a totally connected world, cybersecurity has become a major issue. It encompasses a range of technologies designed to protect computers and networks from unwelcome intrusion and to ensure their continued reliability. The rapidly escalating threats posed by these issues require constant vigilance and education.

Fujitsu is Proud to Deliver an Independent Perspective

To shed light on this issue Fujitsu is proud to deliver to you this independent report on the true state of Cybersecurity in Thailand. Asia/Pacific based research firm Technology & Management Services (TMS) surveyed 107 Thai ICT decision makers in December 2018 and produced this report.

What this Report Covers

The report briefly explains what Cybersecurity actually is, and why it is important. It not only shows the current status of Cybersecurity in Thailand, but also sheds light on organisation objectives and plans for the next 12 months.

Specific topics covered are:

- Cybersecurity & Business Continuity Implementation vs Investment
- Cybersecurity & Business Continuity Progress for Business Operations
- Cybersecurity & Business Continuity Implementation Status - Specific Applications
- Cybersecurity Preferred Provider Location
- Business Continuity Preferred Provider Location

Other reports in the series focus on:

- Key ICT Trends and Digital Transformation
- Workplace/Workstyle Innovation
- Cloud & Internet of Things (IOT)
- Artificial Intelligence (AI)
- Enterprise Applications/ERP

Cybersecurity and Business Continuity are becoming increasingly critical aspects of all business operations. It is important to not only ensure that all levels of access to corporate systems, from individual level through to extra-enterprise level between companies are secured, but that data can be recovered quickly in the event of loss.

From this report it is clear that Thai business leaders have a solid understanding of these issues. It is my hope that you will use the findings in the attached report to further clarify these important technology issues, and that they prove useful in your own planning processes.

Toshio Miura, Managing Director
Fujitsu Thailand Co., Ltd.

Executive Overview and Key Findings

Introduction

In December 2018, TMS conducted the first 'State of The Nation: ICT in Thailand 2019' survey. The result was a highly qualified and reliable set of complete responses from 107 ICT decision makers, regarding current ICT status and future plans. Key findings from *'Report 4: Cybersecurity'* follow:

Key Findings:

- The majority of respondents agree that cybersecurity is important, with a bias towards it being marginally underhyped.
- Cybersecurity is a priority in most organizations as corporate networks become more diverse and distributed, as indicated by the high investment and implementation in securing the cloud, antivirus/spyware and data encryption. These three areas also already have the highest levels of existing investment.
- In terms of business continuity, investment in mission critical back-up and recovery, redundant sites, cloud backup is also moderate, with future investment also planned.
- Most respondents stated that they were making progress with programs that were well underway or mature and outcomes delivered in the areas of operations (72%), finance (71%), and marketing (70.1%).
- In terms of specific cybersecurity application implementations antivirus/spyware applications ranked number one with 84.1% of respondents well underway or significant outcomes delivered.
- The geographic source of cybersecurity provider was important to respondents, with 33.6% preferring ed a global provider and 29% preferring d a blend of local/regional and global players.
- For business continuity provider source in terms of geographic location 29.9% preferred regional players, closely followed by global players at 29%.

Thai Business Leader Responses

Cybersecurity and Business Continuity are becoming increasingly critical aspects of all business operations. It is important to not only ensure that all levels of access to corporate systems, from individual level through to extra-enterprise level between companies are secured. Once secured, it is even more critical to ensure that essential mission critical data is appropriately backed up, and able to be restored in a timely manner.

Failure to establish and regularly test processes to ensure security and business continuity can result in the complete inability to conduct business and will have long-lasting impacts on business viability in general. Thai business leaders have a solid understanding of these issues, have already invested heavily in the critical components of these two related areas and are planning further investment. This is especially true of antivirus/spyware, data encryption and mission critical backup and recovery, including redundant site operations.

Cybersecurity

Cybersecurity Covers All Computer Access

What used to be called computer security is now most commonly called cybersecurity. The change in terminology reflects the evolution from discrete to interconnected computer systems. It is only since computers have been connected to each other that issues around protecting them from unwanted intrusion become prominent.

Individual to Enterprise and Nation State

Cybersecurity has many parts, from the protection of individual devices to the protection of the enterprise and even the nation state. One important aspect is identity and access management, a range of technologies intended to ensure that only validated individuals have access to the appropriate levels of information. Identity management systems are now being implemented at the national level with the increasing popularity of e-government systems.

Biometrics

Many identity management systems include a biometric component, using voice or facial recognition, fingerprints, and other distinctive physical attributes to verify and identify individuals.

SIEM

The term SIEM (Security Information and Event Management) is the term increasingly being used to describe the range of techniques and technologies employed to ensure that enterprise Information systems are secured from outside interference. Such interference can come from individuals, organised crime groups, other enterprises, or even nation states. They can be motivated by revenge and thrill seeking in the case of individuals, or by financial advantage in the case of access to proprietary information.

SIEM systems are the fastest-growing and most important product area in Cybersecurity. They have three major components:

- **Data collection:** gathering data about system activity from syslogs, firewalls, application monitors, and operating system and network traffic logs.
- **Data analysis:** log management and retention, event correlation, user activity monitoring, and predictive and forensic analysis.
- **Reporting:** real-time dashboard alerts, email and SMS with alerts, analytical reporting, auditing and governance, and compliance.

Cyber Warfare

Cybersecurity is increasingly important to governments, where it is now seen as an area of international conflict. Cyberwarfare is a reality, with nation states as perpetrators as well as victims. Most countries now have national cybersecurity centers, drawing on the capabilities of private industry, government and academic specialists in the area.

A New Arms Race

Cybersecurity is a constant battle of changing technology. There are many excellent point solutions, a range of comprehensive suites and a large services and systems integration industry that provide clients with cybersecurity solutions based on a range of products. However malicious players are constantly employing new techniques and technologies. It is a new arms race, and there is no one size fits all solution.

The TMS Technology Hype-Dial: What's Hot and What's Not!

The TMS Technology Hype-Dial

It is often hard to separate myth from reality in the technology industry. Many technologies are talked about so much that the reality of their importance is lost in all of the noise. To help cut through the disinformation, Technology & Management Services (TMS) has developed the TMS Technology Hype-Dial.

Overhyped, Underhyped, Important or Not Important?

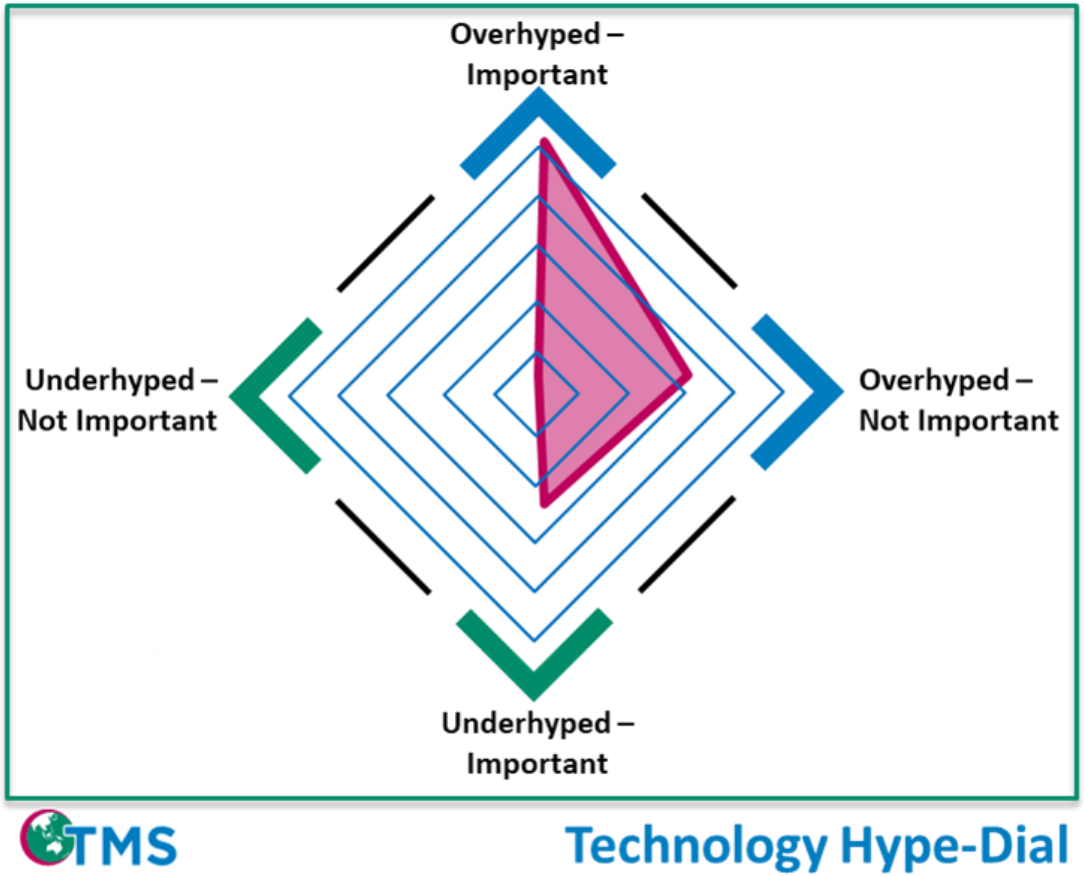
As an integral part of our extensive research process, TMS surveys hundreds of ICT decision makers in specific markets. We ask respondents to rate a number of technologies or business trends in terms of whether they believe them to be ***overhyped or underhyped***, and whether they are ***important or not***.

The Shape of the Dial Indicates the Level of Reality

Overall results are analysed and expressed as a four-point radar ("spider") diagram for each technology or trend. ***The thinner the shape the more important*** ICT Decision Makers believe the technology to be. ***The higher the shape the more the technology is believed to be overhyped***.

The Hype-Dial Evaluates Technology Based on Merit

The TMS Technology Hype-Dial allows ICT decisions makers to consider or reject a new technology or business trend based on its merits as identified by their peers. ICT decision makers evaluate the benefits of technologies in terms of their enablement of business and ICT objectives, which evolve over time, but which do not change nearly as quickly as technology.



Use Other TMS Tools to Establish Context

The Technology Hype-Dial should be used in conjunction with other TMS tools such as the Implementation & Investment Matric (I^2M) and other TMS charts and graphs. This will assist in establishing the context of these technologies against business and ICT objectives, as well as budget and implementation plans and the associated challenges.

Cybersecurity: Technology Hype-Dials

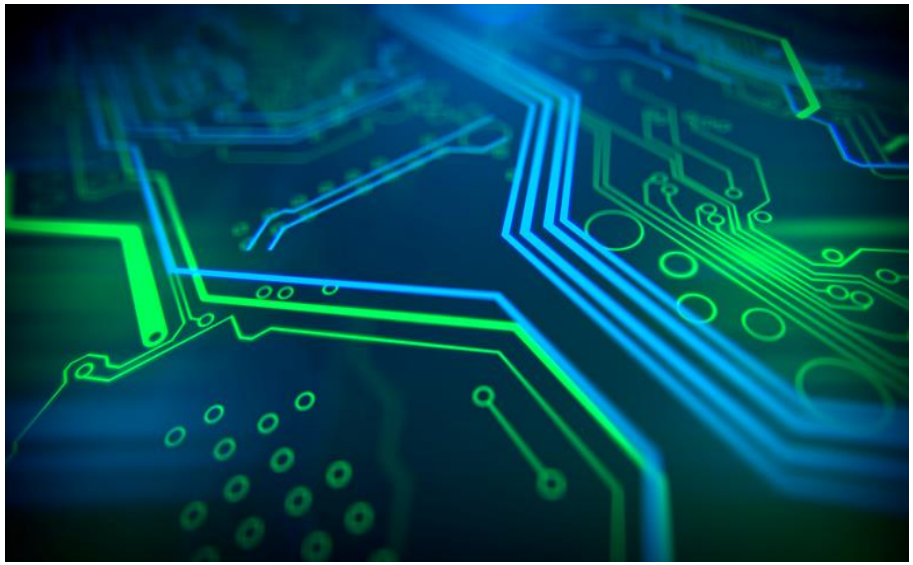
Cybersecurity Hype-Dial

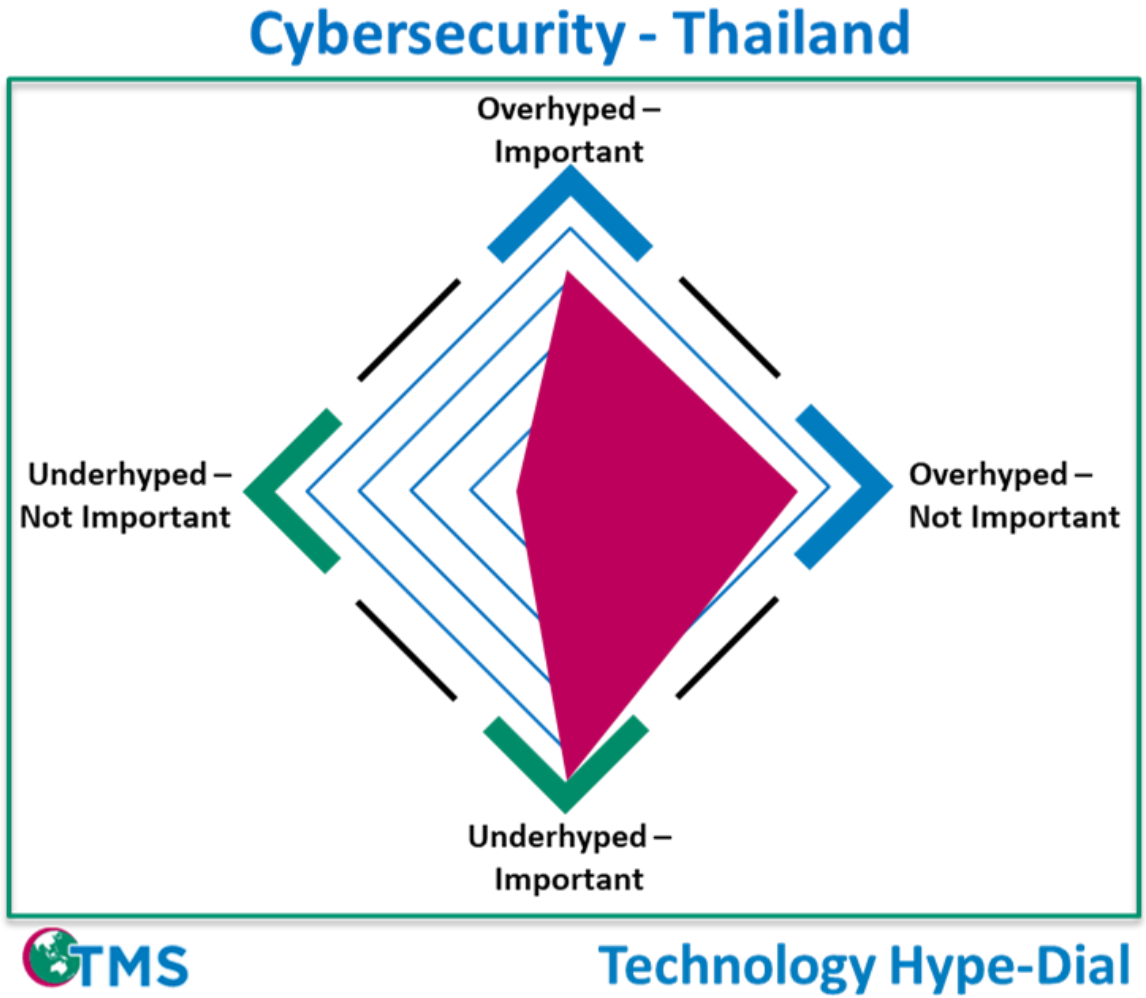
This is an unusually shaped Hype-Dial, with high scores for three points.

The majority of respondents agree that cybersecurity is important...with a bias towards it being marginally underhyped.

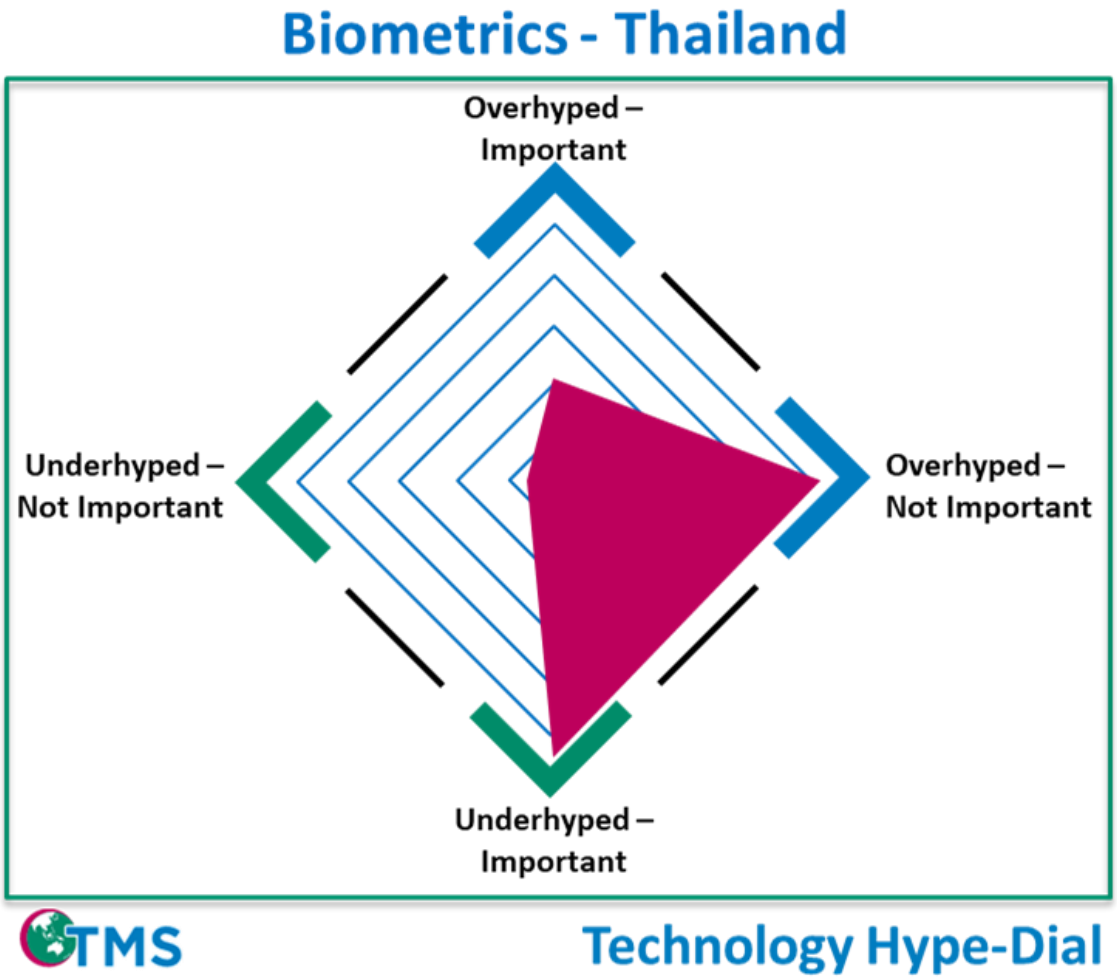
Hoever a large number also believe it to be overhyped and unimportant.

This is potentially an indication that more information about cybersecurity is required to clear up any confusiom about its importance.





Biometrics: Technology Hype-Dials



Biometrics Hype-Dial

Biometrics is one of the key technologies for implementing cybersecurity so we have split this out for further analysis.

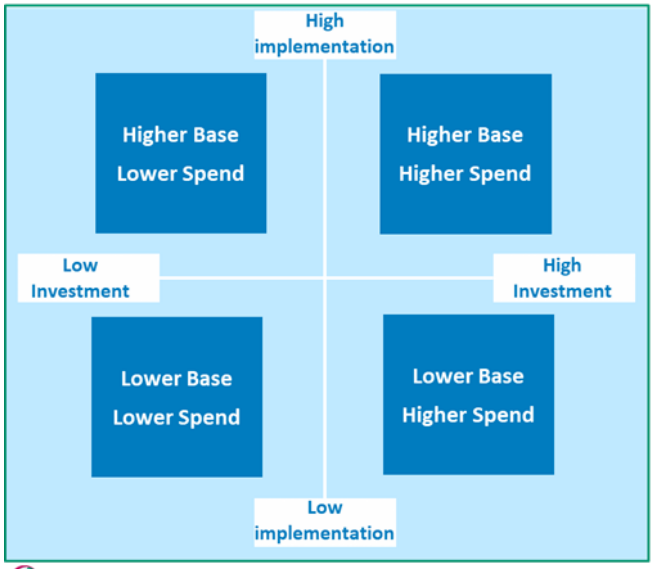
This is a very unusual shaped Hype-Dial in general.

The respondents agreeing that is important is almost equal to those who believe it be unimportant.

In terms of hype, respondents were almost evenly split between it being unimportant or important. With importance being smarginally higher.

The TMS Implementation vs Investment Matrix (I^2M)
What has Been Implemented and What is Planned?

TMS Implementation vs Investment Matrix (I^2M)
When evaluating what technology profile is best for your organization, it is often useful to have information about what other organizations are doing and are planning. To reveal the actual status in your market, Technology & Management Services has developed the TMS Implementation vs Investment Matrix (I^2M).



TMS Implementation vs Investment Matrix (I^2M)

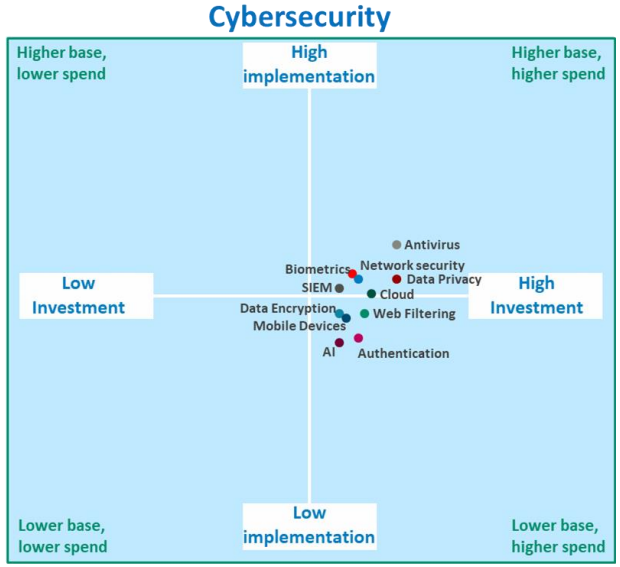
Directly from ICT Decision Makers
As an integral part of our extensive research process, TMS surveys hundreds of ICT decision makers in specific markets. We ask respondents to indicate the level of ***current technology implementation*** (from nothing at all to highly mature) and the level of ***planned technology investment*** (from none-at-all to major investment plans).

Actual vs Planned Technology Use
Overall results are analysed and expressed as a matrix which maps actual implementation (low to high) against planned investment (low to high). The positioning of technologies within the TMS I^2M shows their status relative to each other and is not designed to reflect actual market shares.

TMS I^2M Enables Comparison in One Place
Traditional research analyses often focus on technology market share, market size and forecasts, but this doesn't allow for a useful comparison of the actual organizational level of technology use, or the maturity of organizations' planned technology use. The I^2M allows current and planned implementation and investment for clusters of related technologies to be compared on one chart.

Example Chart for Cybersecurity
The example chart for Cybersecurity shown here (not for any specific market), compares the level of implementation of various Cybersecurity related technologies with the level of planned investment.

Use Other TMS Tools to Establish Context
The TMS I^2M should be used in conjunction with other TMS tools such as the TMS Hype-Dial and other TMS charts and graphs. This will assist in establishing the context of these technologies against business and ICT objectives, as well as budget and implementation plans and the associated challenges.



TMS Implementation vs Investment Matrix (I^2M)

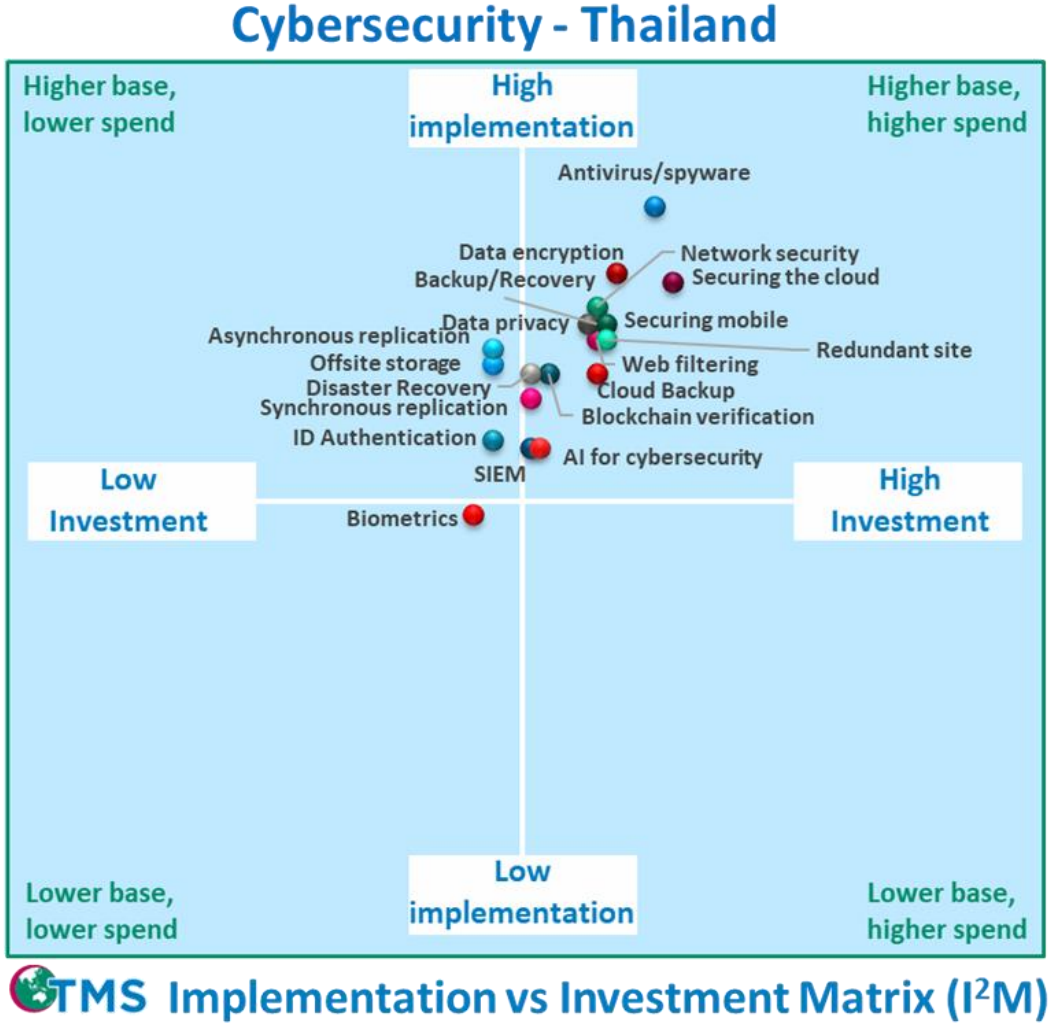
Cybersecurity and Business Continuity: Implementation vs Investment Matrix (I^2M)

Cybersecurity/Business Continuity Implementation vs Investment Matrix (I^2M)

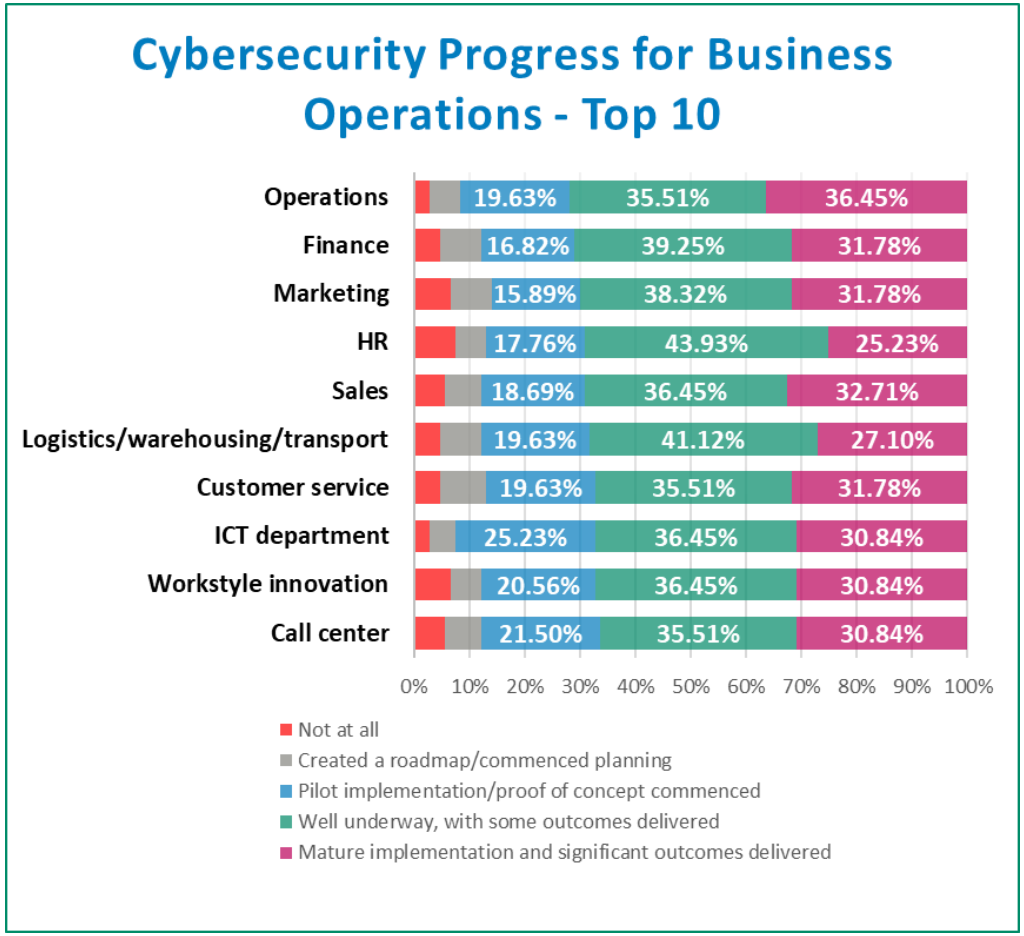
Cybersecurity is a priority in most organizations as corporate networks become more diverse and distributed, as indicated by the high investment and implementation in securing the cloud, antivirus/spyware and data encryption. These three areas also already have the highest levels of existing investment.

A large cluster of technologies also have moderat.ey high levels of investment and are set for further investment. These include, network security, data privacy and securing mobile devisies.

In terms of business continuity, investment in mission critical back-up and recovery, redundant sites, cloud backup is also moderate, with future investment also planned. AI for cybersecurity purposes (such as monitoring, threat analysis via pattern matching, and quarantining) has received some level of investment already but future investment plans are comparatively low.



Cybersecurity: Progress For Business Opeations

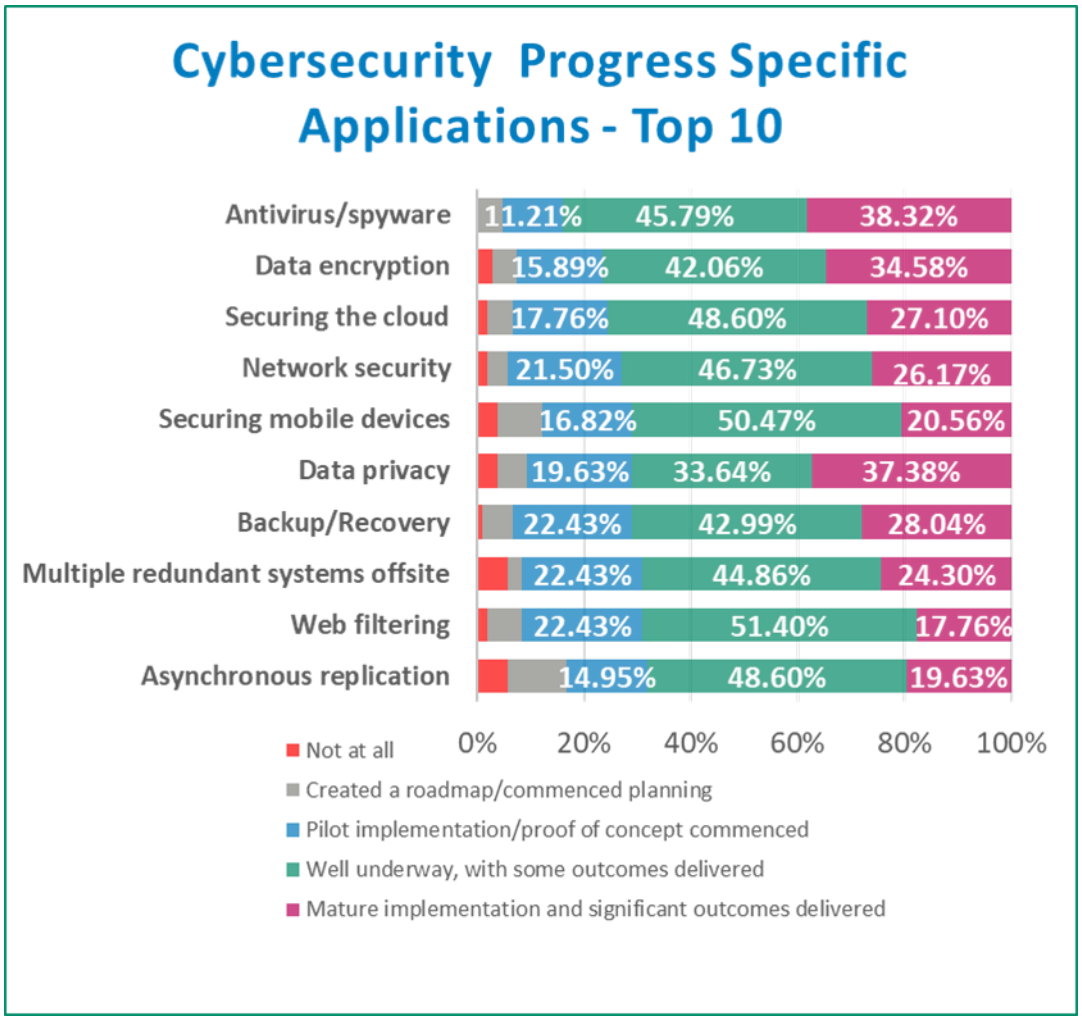


Cybersecurity Progress for Business Operations

We asked ICT decision makers to identify their progress levels for Cybersecurity across 15 key business operations areas. The top 10 are shown here.

Most stated that they were making progress with programs that were well underway or mature and outcomes delivered in the areas of Operations (72%), finance (71%), and marketing (70.1%).

Cybersecurity: Progress For Specific Applications



Cybersecurity Implementation Status - Specific Applications

Cybersecurity implementations span many technologies and applications. We provided a list of 19 and asked respondents to indicate their level of implementation.

Antivirus/spyware applications ranked number one with 84.1% of respondents well underway or significant outcomes delivered.

Data encryption cane in second at 76.6%, with securing the cloud at 75.7% , followed by network security (72.9%).

71% of respondents had also progressed well with securing mobile devices, data privacy and backup/recovery applications.

Cybersecurity: Preferred Provider Location

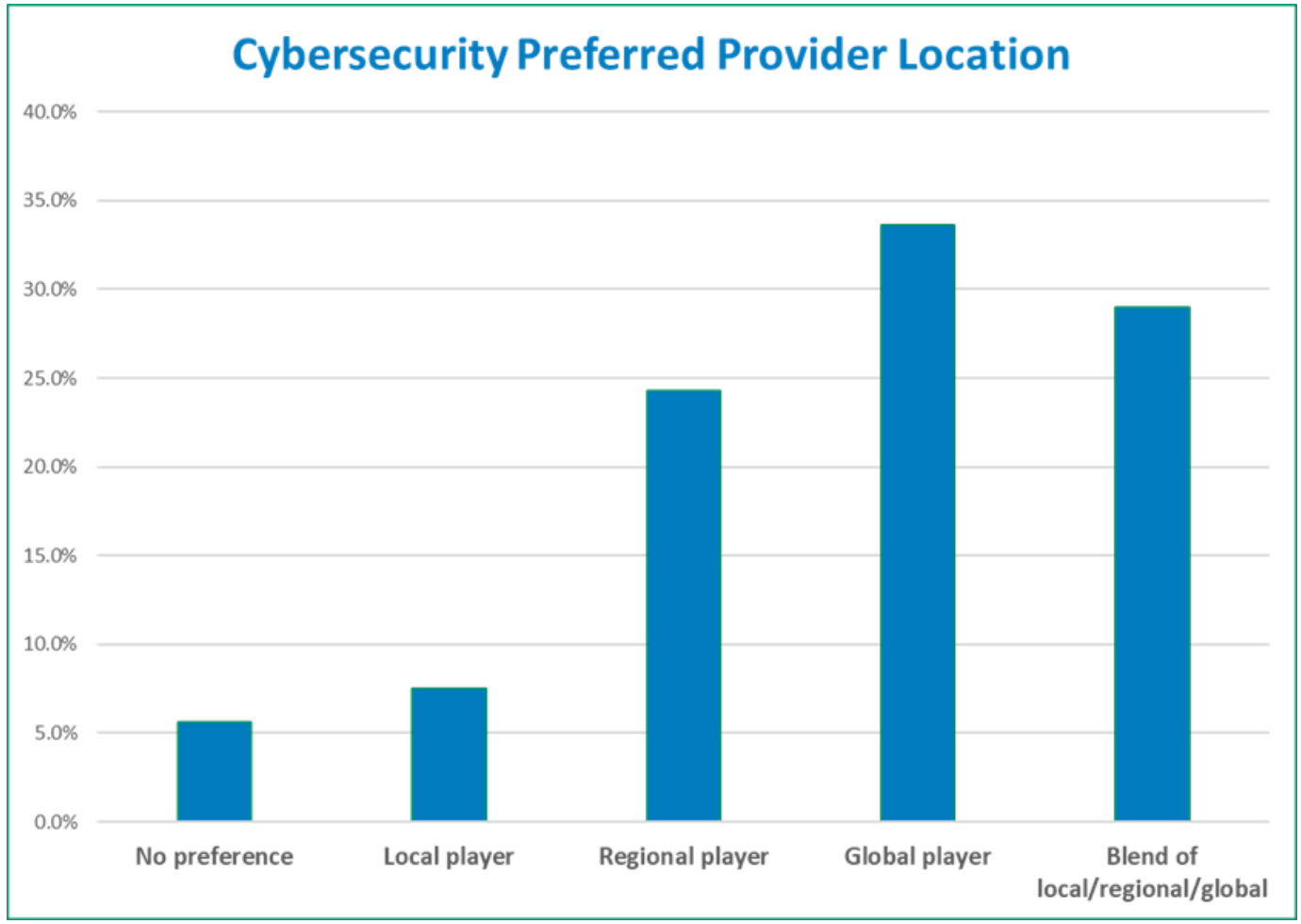
Cybersecurity Preferred Provider Location

We asked respondents what their preferred cybersecurity provider source in terms of geographic location.

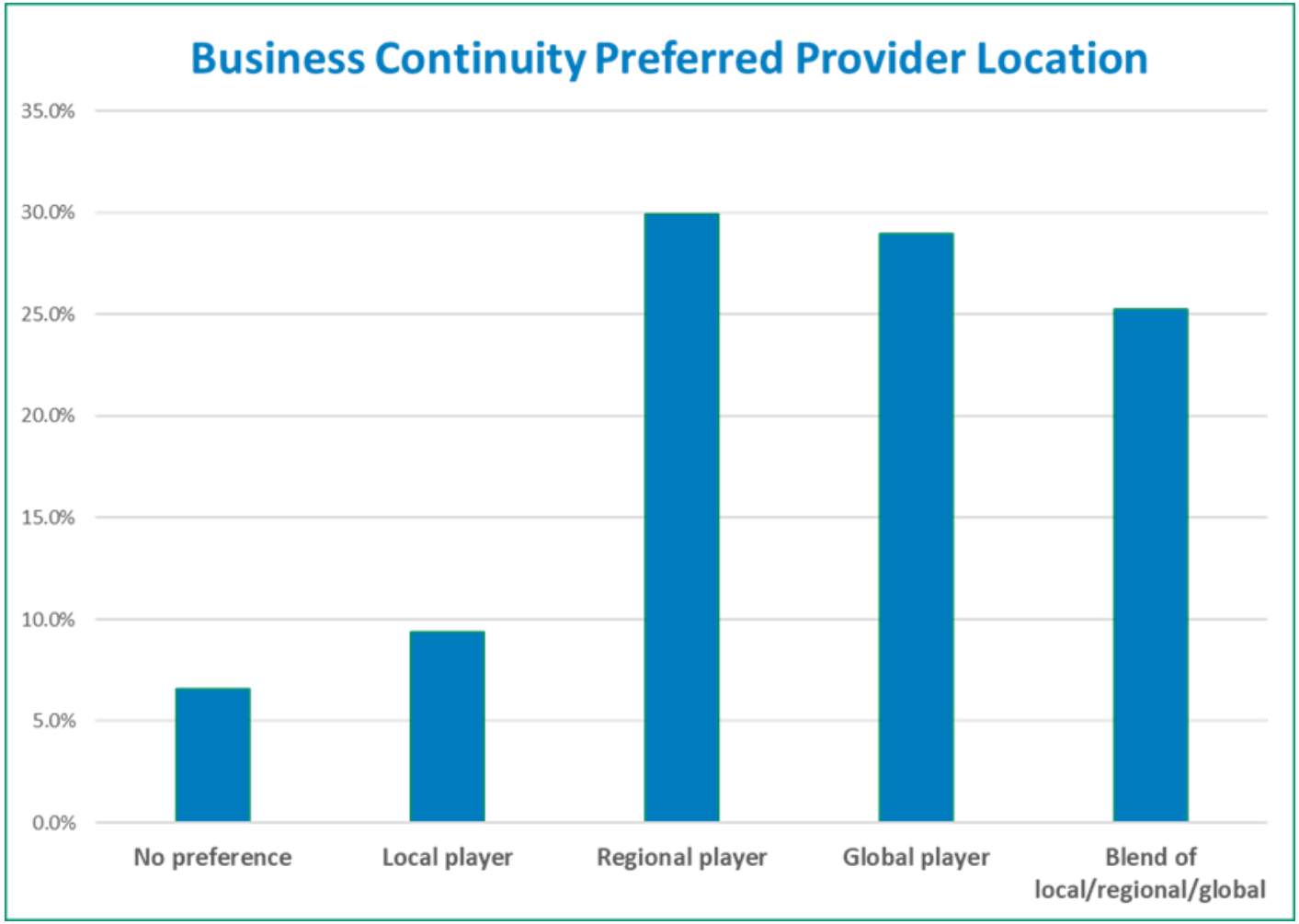
33.6% preferred a global provider.

29% preferred a blend of local/regional and global players, and 24.3% preferred a regional player.

With the remainder preferring a local player (7.5%) or no preference at all (5.6%).



Business Continuity: Preferred Provider Location



Business Continuity Preferred Provider Location

We asked respondents what their preferred business continuity provider source in terms of geographic location.

29.9% preferred a regional player, closely followed by a global player at 29%.

25.2% preferred a blend of local/regional and global players.

With the remainder preferring a local player (9.3%) or no preference at all (6.5%).

Conclusion

Conclusion

What used to be called computer security is now most commonly called cybersecurity. The change in terminology reflects the evolution from discrete to interconnected computer systems. It is only since computers have been connected to each other that issues around protecting them from unwanted intrusion become prominent.

Cybersecurity has many parts, from the protection of individual devices to the protection of the enterprise and even the nation state.

One important aspect is identity and access management, a range of technologies intended to ensure that only validated individuals have access to the appropriate levels of information. Identity management systems are now being implemented at the national level with the increasing popularity of e-government systems.

Many identity management systems include a biometric component, using voice or facial recognition, fingerprints, and other distinctive physical attributes to verify and identify individuals.

The term SIEM (Security Information and Event Management) is the term increasingly being used to describe the range of techniques and technologies employed to ensure that enterprise information systems are secured from outside interference. SIEM systems are the fastest-growing and most important product area in Cybersecurity. They have three major components:

- **Data collection:** gathering data about system activity from syslogs, firewalls, application monitors, and operating system and network traffic logs.
- **Data analysis:** log management and retention, event correlation, user activity monitoring, and predictive and forensic analysis.
- **Reporting:** real-time dashboard alerts, email and SMS with alerts, analytical reporting, auditing and governance, and compliance.

Cybersecurity is a constant battle of changing technology, and malicious players are constantly employing new techniques and technologies. It is a new arms race, and there is no one size fits all solution.

Thai Business Leader Responses

Cybersecurity and Business Continuity are becoming increasingly critical aspects of all business operations. It is important to not only ensure that all levels of access to corporate systems, from individual level through to extra-enterprise level between companies are secured.

Once secured, it is even more critical to ensure that essential mission critical data is appropriately backed up, and able to be restored in a timely manner.

Failure to establish and regularly test processes to ensure security and business continuity can result in the complete inability to conduct your business and will have long-lasting impacts on business viability in general.

Thai business leaders have a solid understanding of these issues and have already invested heavily in the critical components of these two areas and are planning further investment. This is especially true of antivirus/spyware, data encryption and mission critical backup and recovery, including redundant site operations.

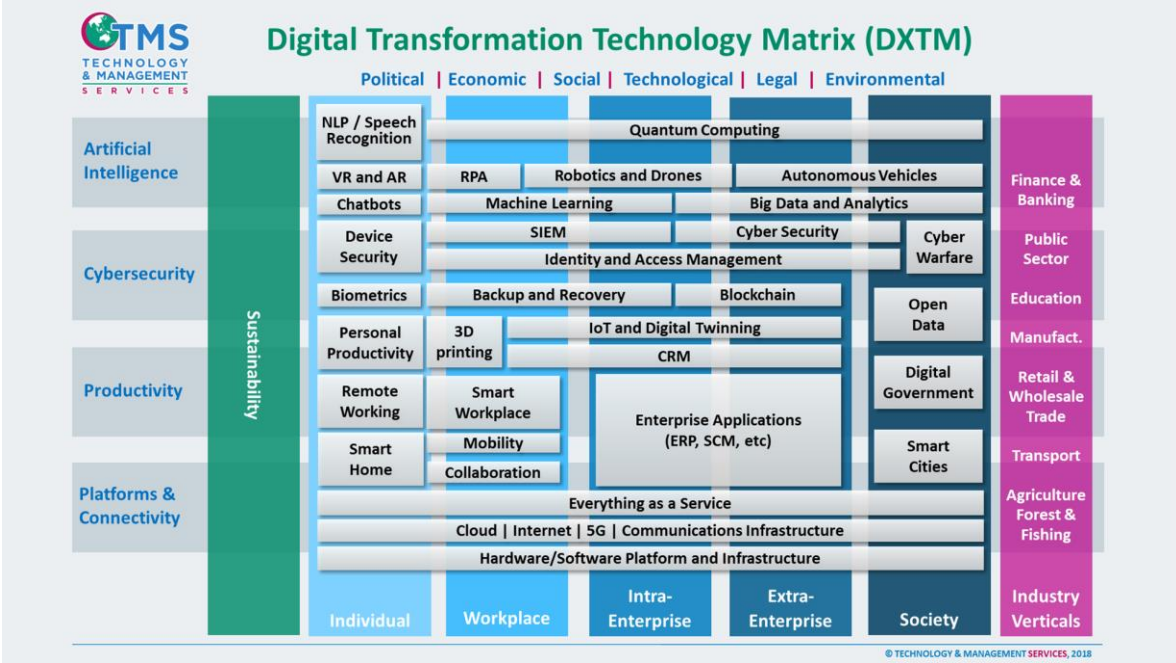
TMS Digital Transformation Technology Matrix (DXTM)

TMS Digital Transformation Technology Matrix (DXTM)

Technology & Management Services (TMS) has developed a proprietary taxonomy of technologies and trends to ensure consistency of terminology. The TMS Digital Transformation Technology Matrix (DXTM) provides a comprehensive model for our research focus.

DXTM comprises **five user groups**, from individual to the wider society:

- **Individual**: The effect of Digital Transformation on individuals, at work and in their personal lives.
- **Workplace**: The effect of Digital Transformation on individuals and workgroups within the workplace.
- **Intra-Enterprise**: The effect of Digital Transformation on business practices and business models within the organization.
- **Extra-Enterprise**: The effect of Digital Transformation on the way the organization interacts with other organizations.
- **Society**: The effect of Digital Transformation on the economy, government and the wider community.



Overlaid on these five groups are **four major classes of application or technology**. Some of these have their primary effect on only one level, some affect two or more. The four technology areas are:

- **Platforms & Connectivity**: Technologies which enable individuals and organizations within each level to communicate and interact with others at their level and beyond. At the base are the underlying connectivity technologies – Cloud / Internet / 5G / Comms infrastructure/Hardware & Software Platforms – which sit across all five user groups and are the key enablers of the interconnected world at every level.
- **Productivity**: Technologies which enable and increase the productivity across functions at every level and across levels.
- **Cybersecurity**: Technologies which prevent unwanted intrusions, and which enable the efficient and continued operation of the other technology areas.
- **Artificial Intelligence**: Machine based technologies which enable new applications through the simulation of human reasoning.

Sustainability/Corporate and Social Responsibility (CSR) are increasingly critical considerations at all levels, and this aspect also overlays the four major classes of application and technology.

Industry Verticals have differing levels of technology uptake and maturity and are therefore specifically included in the research focus.

TMS Research Approach Based on DXTM

TMS Research Approach

The TMS Digital Transformation Technology Matrix (DXTM) enables TMS to clearly identify key technologies and the groups they affect. We discover the trends in each area through primary research – comprehensive and intensive large-scale surveys of ICT decision makers across major industry sectors.

Demographic analysis then allows us to measure and compare the effect of each technology in each industry sector, and also to compare their impact across different sizes of organization and different countries.

Primary research of this nature is based on what the users of the technology are thinking and doing. This quantitative analysis is complemented by qualitative research based on interviews with key players in the user and vendor communities.

This proven methodology offers insights simply not available with secondary research. It is the users of technology that ultimately determine the success and speed of its implementation.

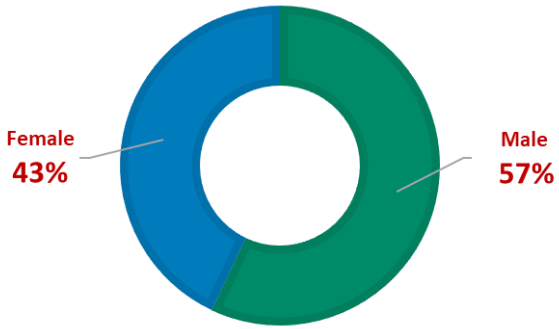
When predicting futures there is no substitute for asking the users of the technology about their attitudes, behaviours and intentions.

Demograpics

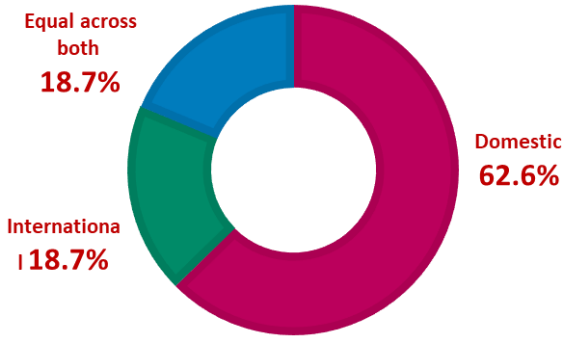
Exhaustive Data Collection Process and Demographics

Almost 10,000 potential respondents were contacted across Thailand, with the aim of identifying over 100 key ICT Decision makers. TMS applied 7 levels of exhaustive screening and validation questions, then conducted extensive data scrubbing, and removal of non-representative data and outliers. The result was a highly qualified and reliable set of complete responses from 107 ICT decision makers. These responses have been summarised in the attached report. Key demographic splits are shown below.

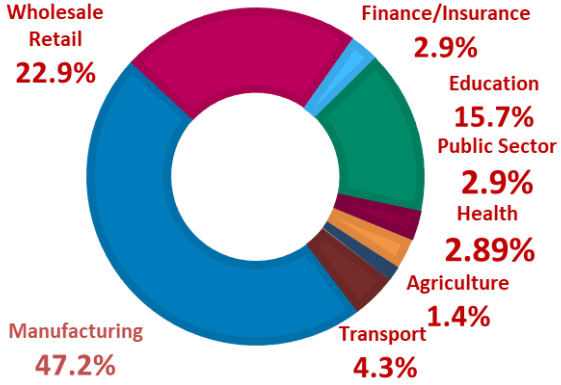
Gender



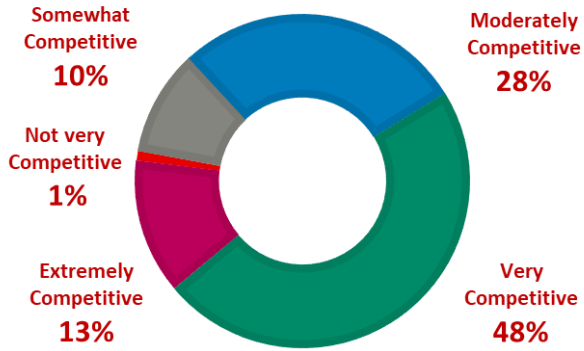
Competition Source



Industry Breakdown



Competition Intensity



How to Contact Us

Acknowledgement to ICT Decison Makers

TMS would like to thank the many hundreds of people and organizations involved in the production of this report. We would particularly like to thank the ICT decison makers/CIOs and senior IT managers who responded to the survey upon which it is based. We appreciate the many time constraints they face, and without their assistance the exercise would not have been possible.

About Fujitsu

Fujitsu is the leading Japanese information and communication technology (ICT) company, offering a full range of technology products, solutions and services. Approximately 140,000 Fujitsu people support customers in more than 100 countries. We use our experience and the power of ICT to shape the future of society with our customers**.** Fujitsu Limited (TSE:6702).

For further information, please see http://www.fujitsu.com

Copyright information

About Technology & Management Services (TMS)

Technology & Management Services is an Asia/Pacific based Research and Advisory services company specialising in the areas of ICT Strategy for technology users and providers, Research-based Thought Leadership, Market and Competitive Intelligence, and Marketing and Technology Strategy consulting projects.

TMS is also highly experienced in the area of Cross-Cultural Communications and Leadership, Managing Virtual Teams across multiple geographies, and runs training and workshops in these areas. In addition TMS's associates are skilled at the delivery of presentations at events ranging from facilitation of small C-level roundtables, through to 'big-tent' major keynotes with audiences in the thousands.

With a combined ICT market experience of over 120 years, TMS associates have supported hundreds of ICT providers and other private and public sector organizations. TMS has successfully executed projects globally, but has a particularly strong focus on Asia/Pacific and Japan.

TMS TECHNOLOGY & MANAGEMENT SERVICES

For further information email: Info@techandmanagementservices.com

STATE OF THE NATION