Data Driven

STATE OF THE NATION SERIES

Delivered to you by:

FUJITSU

ICT in Thailand 2020

Cybersecurity Trends

STATE OF THE NATION

Table of Contents

Foreword	3
About the Report	4
Executive Overview and Key Findings	5
Cybersecurity and Related Topics	6
Cybersecurity Hype-Dial	8
ICT Strategic Challenges and Security	10
Cybersecurity Progress for Business Applications	11
Security Technology Implementation vs Investment	12
Security Applications Implementation vs Investment	14
Security Related Services Implementation vs Investment	15
Business Continuity Services Implementation vs Investment	16
AI for Security Implementation vs Investment	17
Cloud Selection Criteria and Security	18
Preferred Origin of and Satisfaction with Providers	19
Conclusion	20
DataDriven Digital Transformation Technology Matrix (DXTM) & Research Approach	21
Demographics	23
About Fujitsu and DataDriven	24

Foreword

DataDriven State of The Nation: ICT in Thailand 2020

This report is based on our second large-scale survey of ICT decision makers in Thailand. It is a drill-down into the area of Cybersecurity and related technologies and services through the eyes of the people who actually manage and deliver these technologies – the ICT decision makers.

Cybersecurity has many complex facets

Because cybersecurity is everywhere, it has many facets. Point solutions are still common, but most organizations with a comprehensive cybersecurity strategy have a adopted a more integrated approach. There is no one size fits all solution, and every organization will need a different combination of cyber security products and services.

Cybersecurity is also becoming very important to governments, where it is increasingly seen as an area of international conflict. Cyber warfare is a reality, with nation states 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.

It is a constant battle of changing technology. Malicious players are constantly employing new techniques and technologies, and ICT faces new challenges daily.

Fujitsu is Proud to Deliver an Independent Perspective

The technology and services available to meet mission critical enterprise wide security needs of organizations is changing dramatically as are the delivery and commercial models and new challenges arise daily.

To shed light on these challenges Fujitsu is proud to deliver to you this independent report on the true state of Cybersecurity and related services in Thailand. Asia/Pacific based research firm DataDriven surveyed 125 Thai ICT decision makers in October 2019 and produced this report.

What this Report Covers

The report provides a comprehensive introduction to Security terminology, technology and concepts and not only shows the current status of Security and related issues in Thailand, but also sheds light on organization challenges, plans and investment for the next 12 months.

Specific topics

- Cybersecurity defined
- Hype-Dial – what is hot and what is not?
- ICT Strategic Challenges and Security
- Cybersecurity progress for business operations
- Security technology implementation and investment
- Security services implementation and investment
- Business continuity implementation and investment
- AI for security plans
- Cloud selection and security
- Security provider preferred geographic origin and satisfaction

Meeting the cybersecurity and business continuity needs of your organization is critical, however the rapidly changing and increasingly dangerous security environment has increased the challenges for today's ICT decision maker.

Fortunately, the range of cybersecurity offerings and related services also continues to increase at a similar rate, however this has also increased the range of choices. We trust that this report will go some way towards clarifying these issues and augmenting your understanding of what your peers in Thailand are actually doing in this area.

About the DataDriven State of the Nation Report ICT in Thailand: Cybersecurity Trends 2020 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. DataDriven an ICT research and advisory firm with a specific focus on Asia/Pacific surveyed ICT decision makers in Thailand.

After fielding surveys to thousands of potential respondents, DataDriven were able to collect high quality, valid completed responses from 125 ICT Decision makers in Thailand

ICT Decision Makers Need Clarity

As the pressure for *Digital Transformation* increases, ICT decision makers often don't have time to cut through multiple, confusing, conflicting and biased sources of advice.

To provide some clarity, this report series provides detailed analyses of the *Cybersecurity and related technologies and services market* in Thailand.

Cybersecurity and Related Technologies and Services Challenges and Investment Plans

The report places the research into the context of *Challenges, current Implementation levels and Investment directions, and progress of security initiatives* for all major business operations areas for a range of security and related technology areas.

This includes hype levels, security technologies, security for applications, security services, business continuity,AI use for security purposes and security consideration for cloud selection. The preferred source of providers and overall satisfaction with providers are also covered.

A Unique Report Series

This report is the second phase of what we believe to be the first survey of this scope and size conducted in Thailand. This report is part of a series which covers almost every aspect of current and future ICT plans and issues across a wide range of technology and business topics.

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 the area of cybersecurity in Thailand now and for the next 12 to 18 months.

DataDriven DX Technology Matrix and Methodology

Complete details of the DataDriven 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.

Executive Overview and Key Findings

Introduction

In late 2019 DataDriven conducted the 'State of The Nation: ICT in Thailand 2020' survey (this followed a similar survey published in December 2018 2019). The result is a highly qualified and reliable set of complete responses from 125 ICT decision makers regarding current ICT status and future plans. Key findings from the new report *'Security Trends in Thailand, 2020'* follow:

Key Findings

- ICT decision makers encounter many ICT and related challenges. Surprisingly, out of the top 12 challenges, security related issues appeared ten times. This shows the extreme importance of all aspects of security in today's ICT environment.
- Fraud prevention/payment security (92.8%) and cloud security (89.6%) are the hottest areas. Cloud, business and data security are the next most significant at 88.6%, as is optimizing and controlling costs with the same response level. The next 6 challenges also relate to security or privacy with no responses lower than 80.6%.
- Most respondents stated that they are making progress with programs that are well underway or mature and outcomes delivered in the areas of the ICT department (79.2%), Sales (76.8%), operations (76.8%), and call center (75.2%).
- Cybersecurity is a priority in most organizations as corporate networks become more diverse and distributed, as indicated by the very high levels of implementation in antivirus/spyware, data privacy, fraud prevention and encryption. These three areas also already have the highest levels of existing investment.

- A large cluster of technologies also have very high levels of investment and are set for further investment. These include, SIEM, biometrics and blockchain verification
- In terms of implementation, almost all services are at the same level with security analysis, training, managed security and vulnerability testing just leading the pack. These services are closely followed by vulnerability assessment, cybersecurity insurance and forensic services.
- In terms of origin of service providers for cybersecurity technologies most prefer a global player (40%), followed by a blend of local/regional/global (35.2%). 15.2% prefer a regional player and 5.6% a local player.
- 36.9% of respondents are very satisfied with their business continuity providers, followed by 34.5% who are merely satisfied and 27.0% who are highly satisfied.
- For cybersecurity services and implementation, similar scores are evident. 36.9% very satisfied, 31.2% satisfied, and 29.0% highly satisfied.

Thai Business Leaders Responses

Cybersecurity technologies and services are used by almost all organizations in Thailand. Many different types of security initiatives have been implemented at a high level, and investment plans in all areas are aggressive.

Security in the cloud, poses a significant challenge for Thai ICT providers and the criteria for selection of cloud providers now strongly reflects this need.

In general, Thai ICT decision makers are at excellent levels of awareness regarding cybersecurity threats and have implemented quite high levels of technology and invested significant shares of their ICT budget already. However, they are not content with the status quo and continue to invest and prepare for even greater challenges

Cybersecurity and Related Topics

Cybersecurity is the new normal

Cybersecurity is the new normal. What was once a specialised activity is now central to all aspects of information processing. Computer security is no longer an afterthought, something tacked on at the end. It is, or should be, an integral part of systems design and operation.

Because cybersecurity is everywhere, it has many facets. Point solutions are still common, but most organizations with a comprehensive cybersecurity strategy have a adopted a more integrated approach. There is no one size fits all solution and every organization will need a different combination of cyber security products and services. That is all the more reason to adopt a coherent strategy rather than rely on piecemeal tactical fixes.

Cybersecurity is a broad term. It ranges from the safeguard of individual devices to the protection of the enterprise and even the nation state.

A complete cybersecurity taxonomy includes many different product areas. A popular classification is that devised by NIST, the US National Institute of Standards and Technology, which identifies five main categories of cybersecurity, identify, Protect, Detect, Respond, and Recover. This widely used taxonomy identifies the key areas – many cybersecurity products straddle multiple NIST categories.

End-user, endpoint and mobility protection

End user protection systems guard against malware, viruses, spyware, trojan horses and the like at the individual user level. They are typically point products that can be employed by individual users, but which are also integrated into enterprise cybersecurity solutions.

This includes mobile security. Smart phones and other mobile devices are often the preferred interface to many corporate systems. Most endpoint security systems now include mobile cybersecurity functionality. End user applications also need to be secured, particularly those used for collaboration. This includes email workflow, and workplace applications.

Identity and access management

Identity management systems straddle a range of technologies intended to ensure that only validated individuals have access to the appropriate levels of information. They are often 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.

SIEM (Security Information and Event Management)

The range of techniques and technologies employed to ensure that enterprise information systems are secured from outside interference. Such interference can come from individuals, organized crime groups, other enterprises, or even nation states. They can be motivated by revenge and thrill seeking in the case of individuals, financial advantage or by gaining access to proprietary information.

Cybersecurity and Related Topics (Con'td)

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.

Vulnerability management

An important class of cyber security tools and those designed to assess an organizations vulnerability to cyber-attacks. These tools and services include penetration testing and vulnerability assessment, and often include remediation capabilities.

Data center and cloud security

The disciplines of data center security have now been extended to the cloud. Most organizations operate a hybrid environment of in-house and cloud processing. It is important for the whole processing ecosystem to be treated as a single environment for security purposes.

Cloud data center service providers have in most cases implemented sophisticated security practices, but the ultimate responsibility remains with the user.

Data encryption provides an extra level of security and has become a major product set in its own right. Encryption ensures that even if an intruder breaches an organization's security systems, they are unable to use information because it is coded. Encryption and decryption tools have become a significant industry sector.

Cybersecurity services

Many vendors offer specialised cybersecurity services. Some even offer a total solution, from endpoint security to SIEM to disaster recovery and forensic and analysis services. There is also a large specialist cybersecurity training industry.

New technologies

New technologies are constantly changing the cyber security landscape, posing new threats and leading to the development of new products and strategies. Important technologies to the future of cyber security include:

- **Blockchain**: a technology that provides an unalterable audit trail for data. It is increasingly being used in the financial services industry to provide secure transactional systems, though it comes at a cost in performance. Blockchain brings its own cybersecurity challenges.
- **Artificial intelligence**: Covers a range of technologies including machine learning, predictive analytics, pattern matching and behavioural mapping. Many cybersecurity products include AI technologies, but it is also an enabler for hackers and cyber criminals.
- **Internet of Things**: IOT massively increases the number of endpoints in any network, leading to a new class of cyber security products.

A new arms race

Cybersecurity is becoming very important to governments, where it is increasingly seen as an area of international conflict. Cyber warfare is a reality, with nation states 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.

It is a constant battle of changing technology. Malicious players are incessantly employing new techniques and technologies. It is new arms race.

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

The DataDriven 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, DataDriven has developed the DataDriven Technology Hype-Dial.

Overhyped, Underhyped, Important or Not Important?

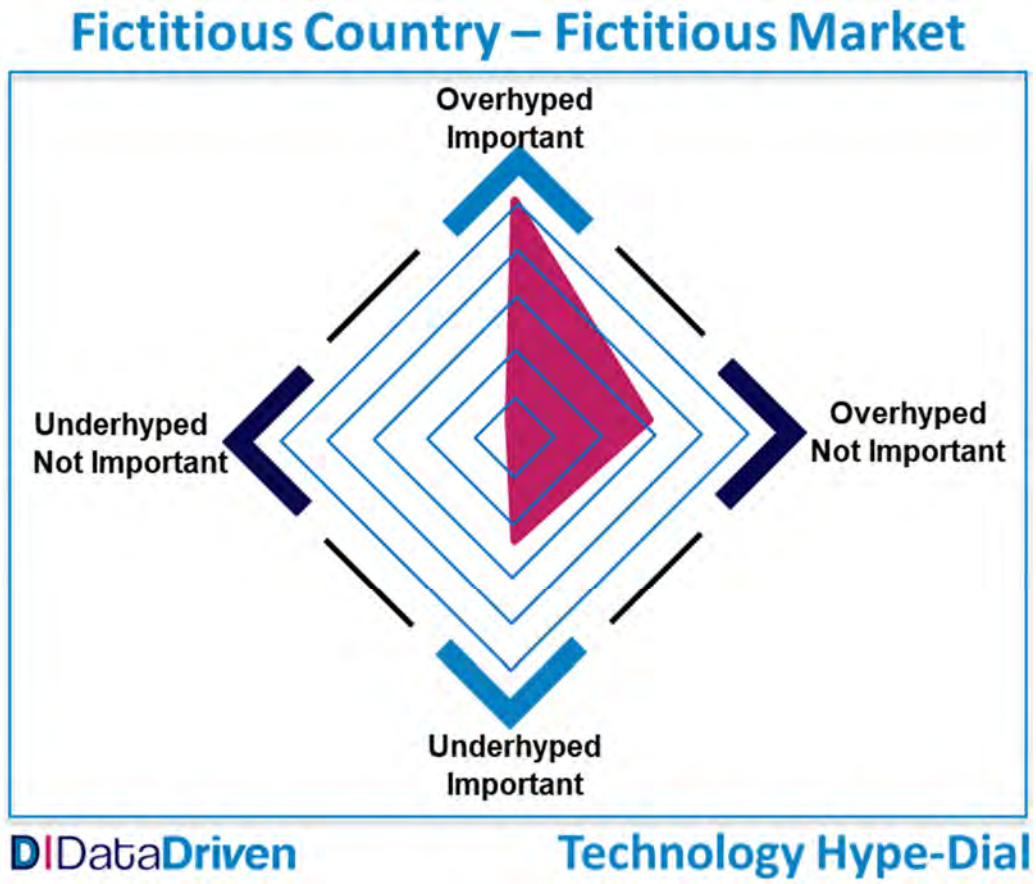
As an integral part of our extensive research process, DataDriven surveys hundreds of ICT decision makers in specific markets. We ask respondents to rate a number of technologies or business trends in terms of whether they believe them to be ***overhyped or underhyped***, and whether they are ***important 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

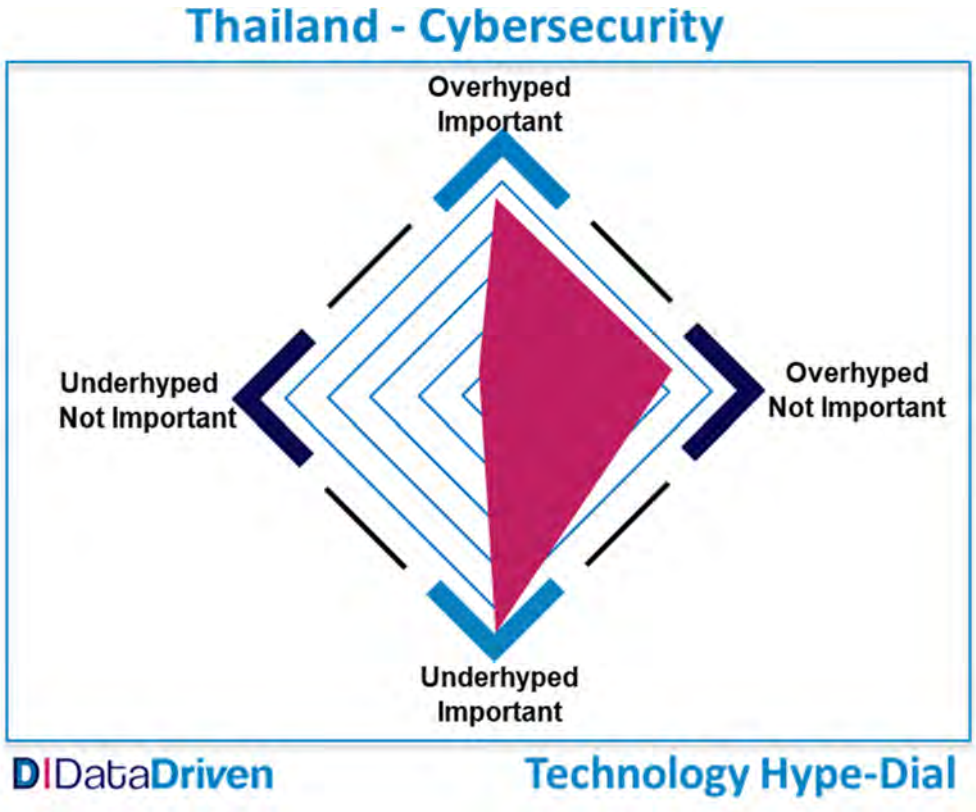
The DataDriven Technology Hype-Dial allows ICT decisions makers to consider or reject a new technology or business trend based on its merits as identified by their peers. ICT decision makers evaluate the benefits of technologies in terms of their enablement of business and ICT objectives, which evolve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



Use Other DataDriven Tools to Establish Context

The Technology Hype-Dial should be used in conjunction with other DataDriven tools such as the Implementation & Investment Matric (I^2M) and other DataDriven 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.

Technology Hype-Dial: Cybersecurity



Cybersecurity Hype-Dial

The area of this hype dial is of moderate to large size compared to most other digital transformation and infrastructure hype dials we have produced.

This dial is pointed more toward the bottom of the dial than usual, indicating that this topic is very important but not hyped enough, i.e. respondents think that there should be more talk about it.

The other two main points of the dial are relatively evenly spread between overhyped and important and overhyped and not important, with a very slight number believing it to be underhyped and not important.

This shape indicates further developments in the cybersecurity area are to be expected as the technology becomes all pervasive.

ICT Strategic Challenges & Security

ICT Strategic Challenges – Top 12

We provided respondents with a comprehensive list of questions (22) about their ICT Strategic challenges and asked them to rank them from highly significant to not significant at all.

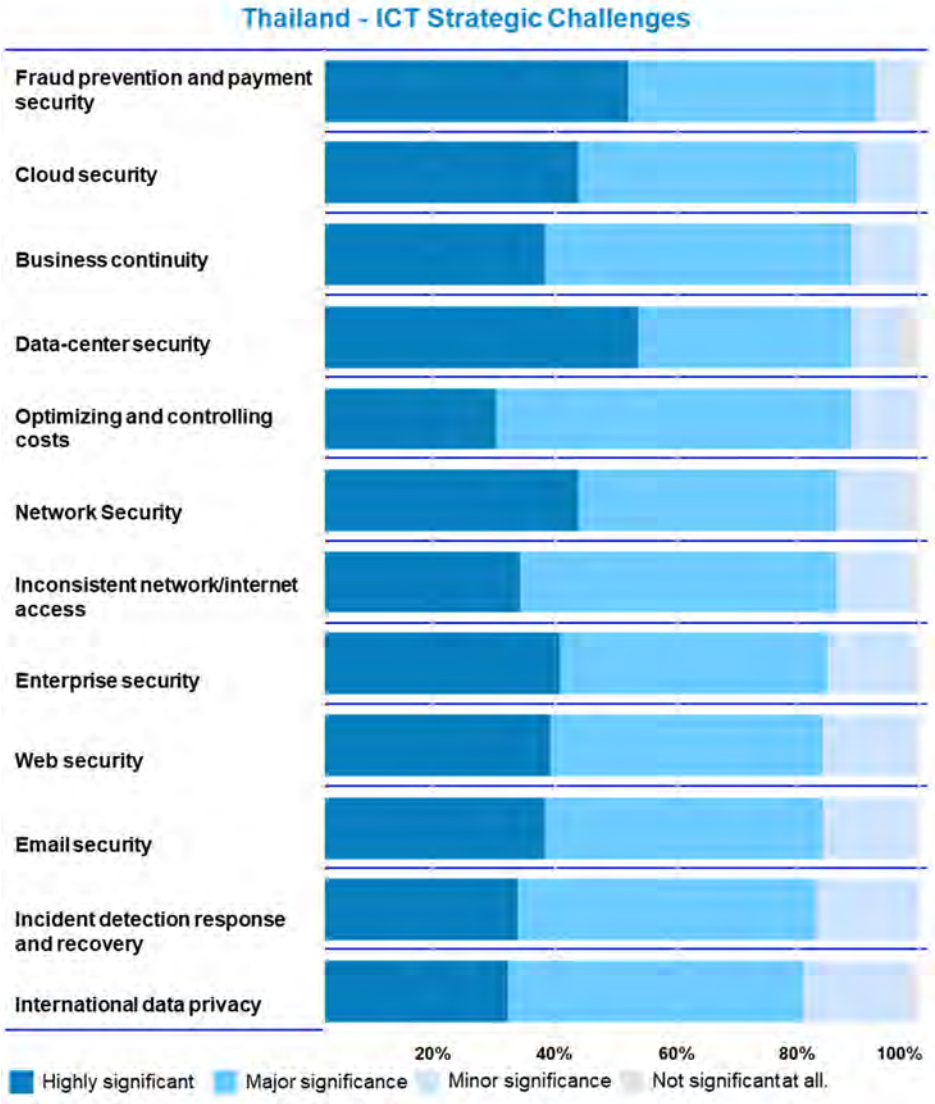
The chart is sorted from the top down in terms of the highest number of combined degrees of challenges (highly significant and major significance).

Surprisingly, out of the top 12 challenges, security related issues appeared ten times. This shows the extreme importance of all aspects of security in today's ICT environment.

Fraud prevention/payment security (92.8%) and cloud security (89.6%) are the hottest areas. Cloud, business and data security are the next most significant at 88.6%, as is optimizing and controlling costs with the same response level. The next 6 challenges also relate to security or privacy with no responses lower than 80.6%.

DX Security Challenges

We asked respondents to rate their digital transformation challenges. 94.4% of respondents indicated that security and privacy concerns are highly challenging or somewhat challenging (grouped), reinforcing the severity level of maintaining secure environments.



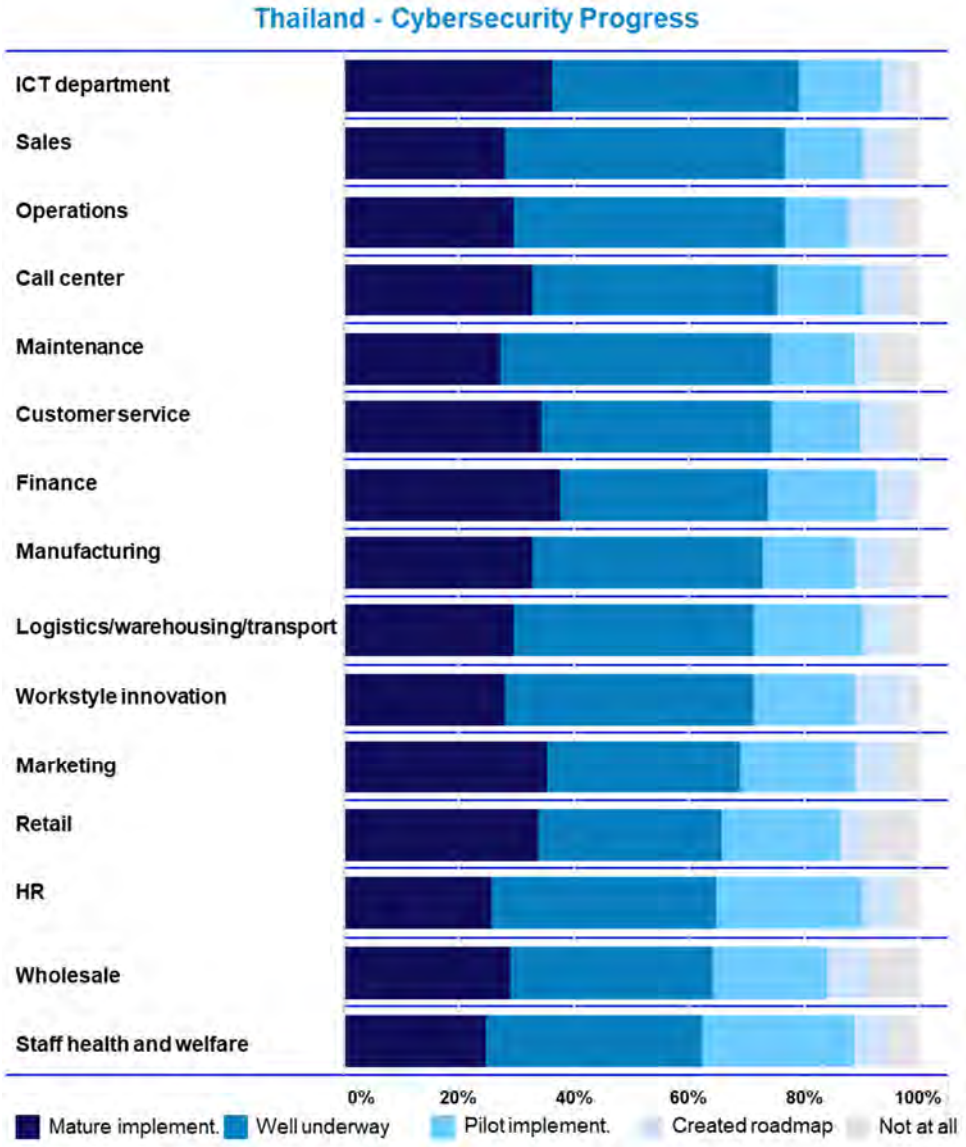
Cybersecurity: Progress For Business Operations

Cybersecurity Progress for Business Operations

We asked ICT decision makers to identify their progress levels for Cybersecurity across 15 key business operations areas.

Most stated that they are making progress with programs that are well underway or mature and outcomes delivered in the areas of the ICT department (79.2%), sales (76.8%), operations (76.8%), and call center (75.2%).

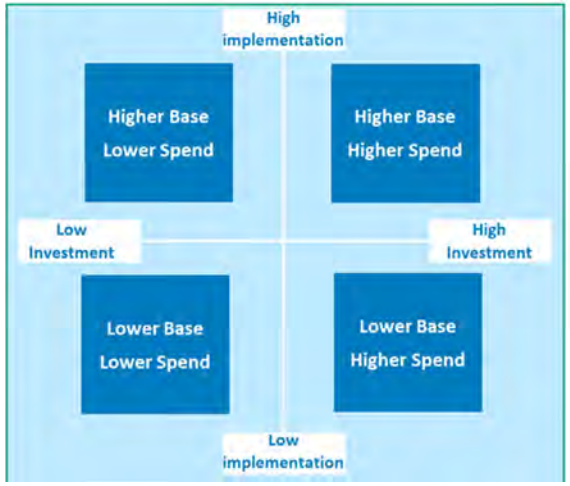
Respondents indicated that they have also made significant process across all other areas as well, with no rating coming in below (62.4%).



The DataDriven Implementation vs Investment Matrix (I²M) What has Been Implemented and What is Planned?

DataDriven Implementation vs Investment Matrix (I²M)

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, DataDriven has developed the Implementation vs Investment Matrix (I²M).



Directly from ICT Decision Makers

As an integral part of our extensive research process, DataDriven 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 DataDriven I²M shows their status relative to each other and is not designed to reflect actual market shares.

DataDriven I²M 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 I²M allows current and planned implementation and investment for clusters of related technologies to be compared on one chart.

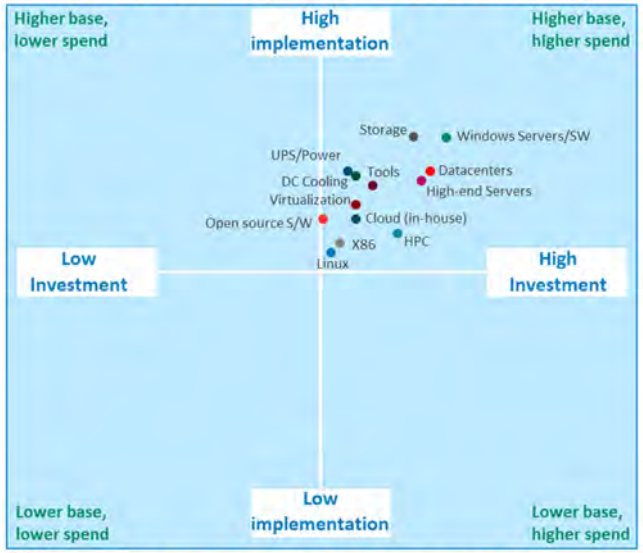
Example Chart for Fictitious Country and Infrastructure Technology

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

Use Other DataDriven Tools to Establish Context

The DataDriven I²M should be used in conjunction with other DataDriven tools such as the DataDriven Hype-Dial and other DataDriven 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.



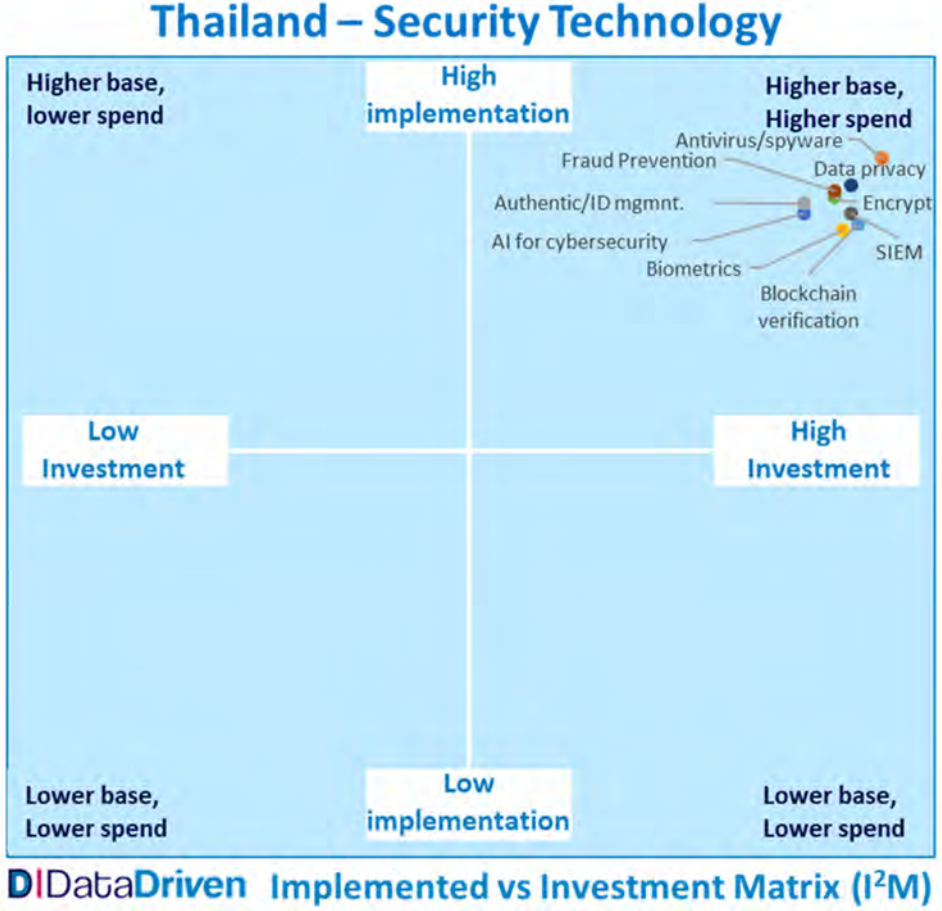
Cybersecurity Technologies: Implementation vs Investment Matrix (I^2M)

Cybersecurity Tech. Implement. vs Invest. Matrix (I^2M)

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

A large cluster of technologies also have very high levels of investment and are set for further investment. These include, SIEM, biometrics and blockchain verification.

Authentication/ID management and AI for security have also been implemented heavily, with future strong investment planned.



Applications Security: Implementation vs Investment Matrix (I^2M)

Applications Security Implement.vs Invest. Matrix (I^2M)

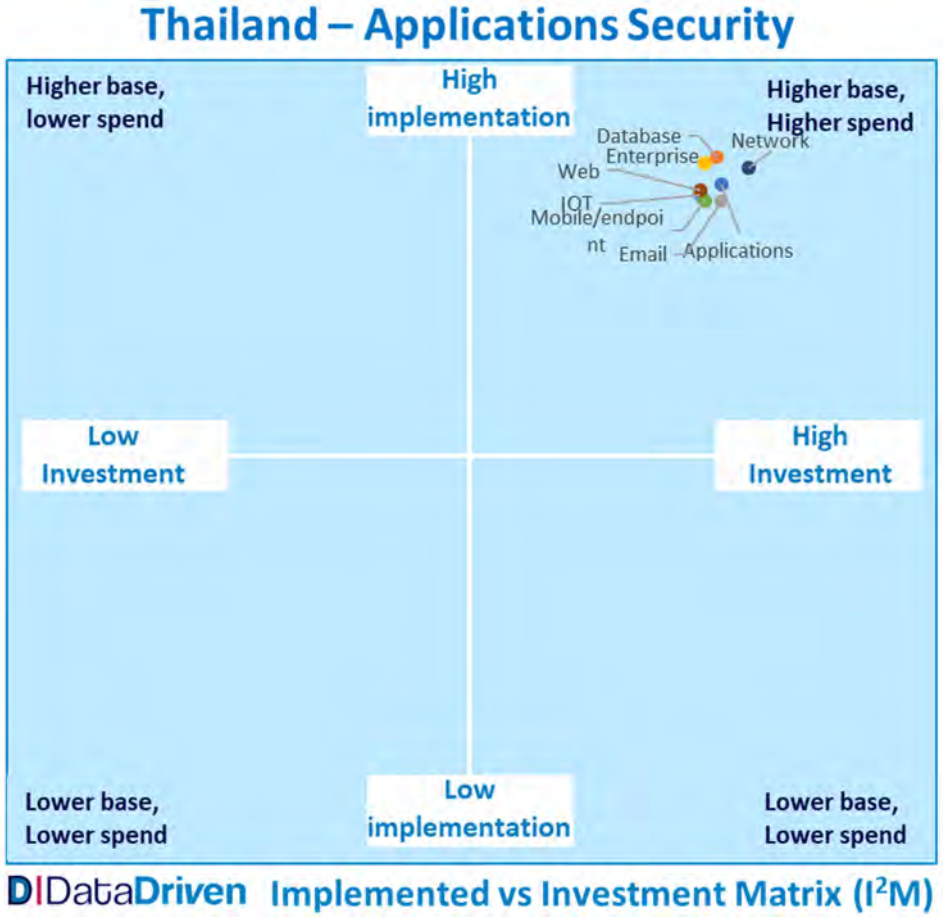
Security designed for specific types of applications is also extremely important in today's ICT environment. This chart shows a wide range of applications being protected.

All technologies surveyed are heavily clustered in the top right, indicating a significant level of implementation and investments.

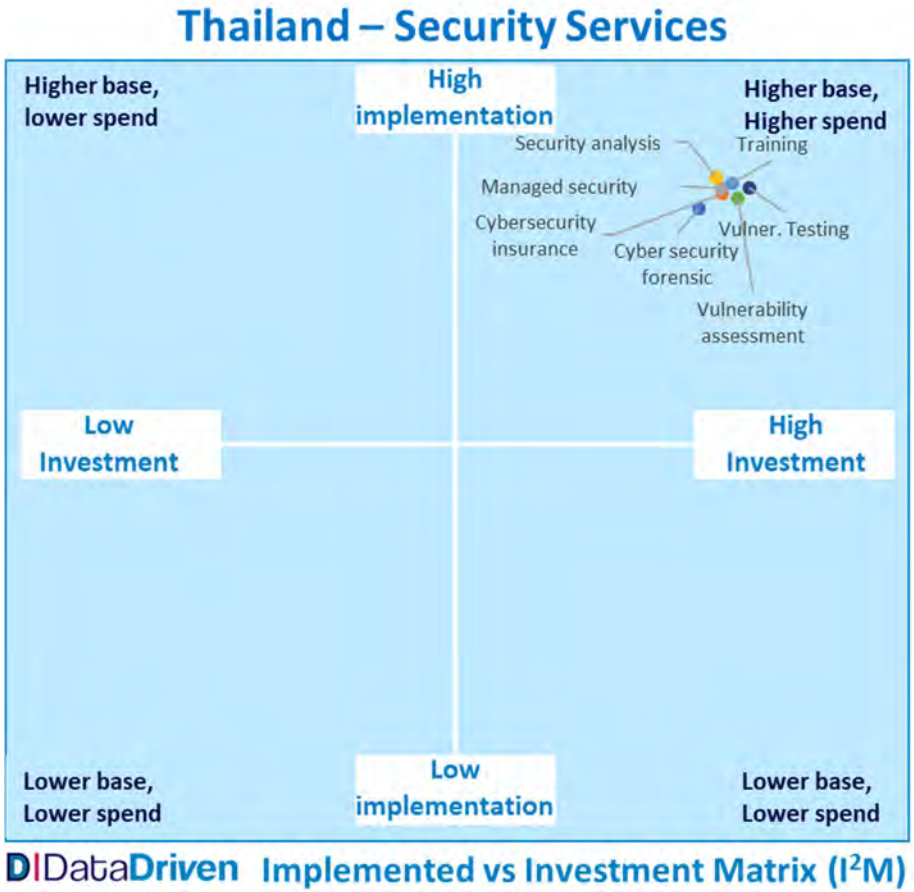
At the top of the implementation list are security applications which secure databases, followed by enterprise wide security, and securing the network.

At the next level, are applications to secure the web, applications processing in general, IOT, mobile endpoint security and email.

All respondents plan to increase investment across all applications related security areas



Security Related Services: Implementation vs Investment Matrix (I²M)



Security Services Implement. vs Invest. Matrix (I²M)

A wide range of services are available to support ICT organizations in their constant quest to secure their environment. This chart shows a high correlation between security technology implementation and investment (as shown in prior charts) and the related services available.

In terms of implementation, almost all services are at the same level with security analysis, training, managed security and vulnerability testing just leading the pack.

These services are closely followed by vulnerability assessment, cybersecurity insurance, and forensic services.

All respondents also plan to invest at high levels across all services areas over the next 12 months.

Business Continuity Services: Implementation vs Investment Matrix (I²M)

Business Continuity Implement. vs Invest. Matrix (I²M)

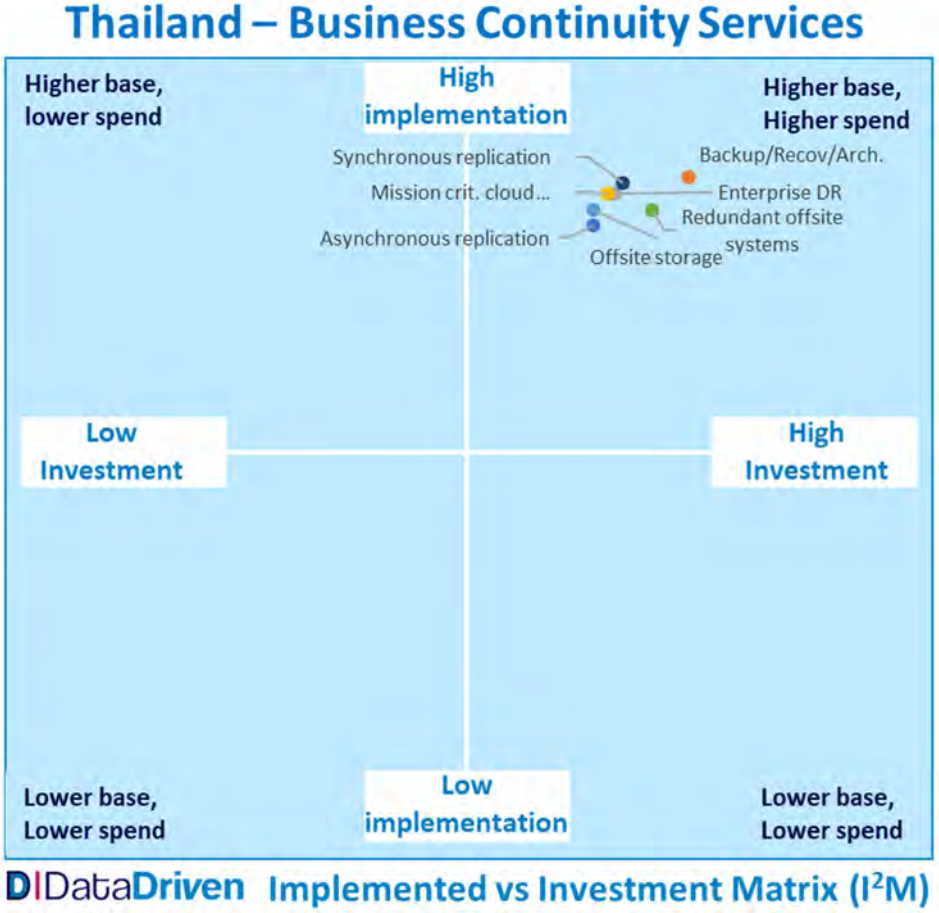
Related to cybersecurity is the important area of business continuity – ensuring that ICT operations continue even in the face of cyber-attacks, natural disasters or other major mishaps.

Important components of business continuity and DRP products and services include:

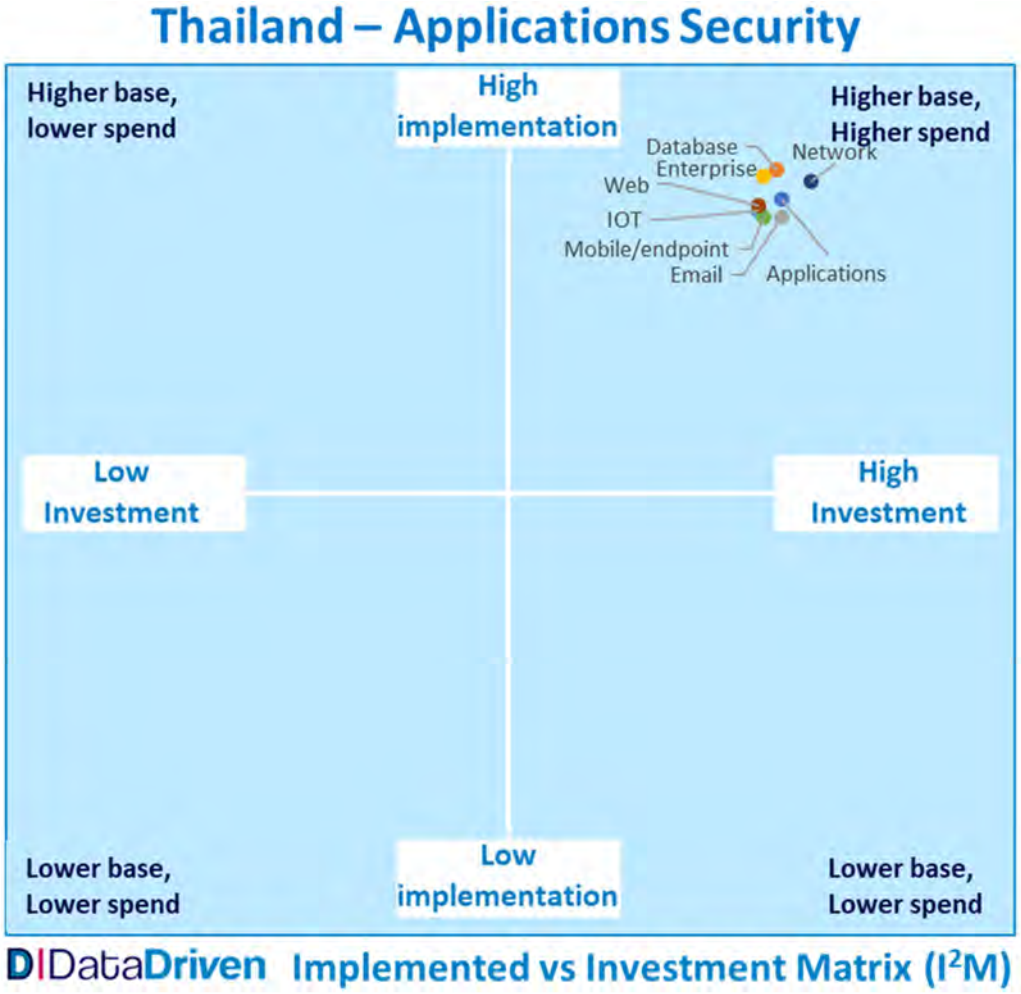
- **Off-site backup and storage**: In the case of catastrophic physical failure of the primary storage system. It often takes place automatically through asynchronous replication. Cloud services providers often provide backup capabilities, but it is ultimately the responsibility of the end user to ensure the integrity of their information.
- **Redundant systems**: Whether processing takes place in house or in the cloud, or a combination of both, it is important to ensure the availability of alternative processing capabilities in the case of cyber-attack or disaster.
- **Disaster Recovery Planning**: DRP is the process of building the policies and procedures to ensure the successful execution of business continuity strategies. It has become a specialist area, often provided by security services providers.

All business continuity initiatives have been implemented at very high levels in particular backup/recovery/archiving, synchronous replication, enterprise-wide DR and mission critical cloud backup. These are closely followed by redundant offsite systems, offsite storage and asynchronous replication.

Most business continuity areas are set to received high levels of investment over the next 12 months, with particularly heavy investment plans for backup/recovery and archiving.



AI for Security: Implementation vs Investment Matrix (I^2M)



AI for Security Implementation vs Investment Matrix (I^2M)

As the scope, damage and pace of security attacks increase in intensity, frequency and creativity, it has become impossible for security to be implemented effectively without some level of machine processing and support.

AI is becoming increasingly important in this escalating battle, with a large number of AI based solutions already being implemented. At the top of the list are authentication processes and cybersecurity specific applications.

These implementations are closely followed by object recognition, facial and voice recognition and pattern recognition which are all essential for threat monitoring, analysis, pattern matching and subsequent quarantining.

All AI based security technologies are set for high investment in the next 12 months.

Cloud Selection & Security

Cloud Selection Criteria and Security

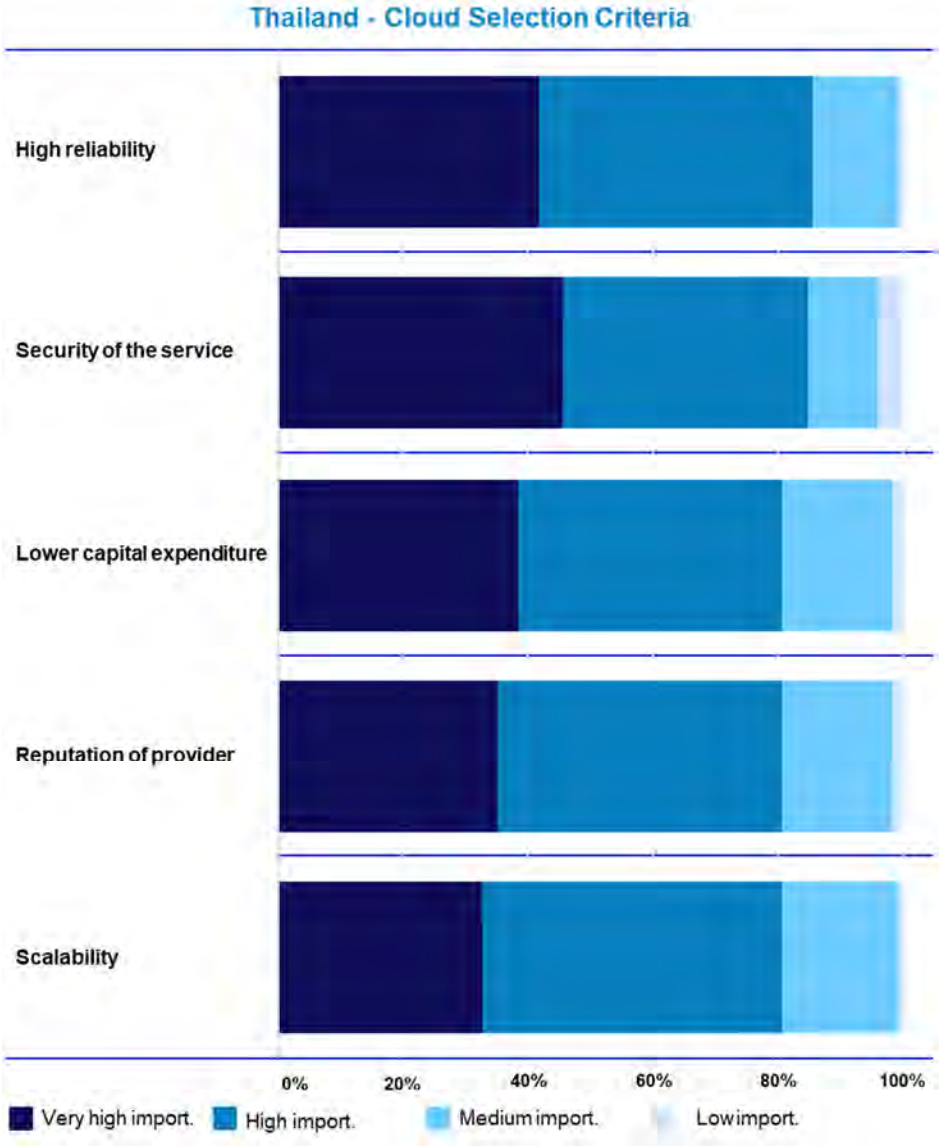
As the use of cloud for mission critical processing increases, it has become increasingly critical to ensure a highly secure environment for cloud.

We listed 10 criteria for the selection of cloud environments.

High reliability came in at the top with 85.6% of respondents, however security of the service came in at an almost equal priority with 84.8% of respondents.

In many prior surveys over the past few years, criteria such as lowering capital expenditure, scalability, ease of operation and ability to change providers are at the top of the list.

The indication from this survey is that securing the cloud (which is also related to reliability) is now becoming the most pressing issue being faced by ICT decision makers in Thailand when selecting cloud processing environments.



Security and Related Topics: Preferred Origin of and Satisfaction with Services Provider

Cybersecurity Preferred Provider Origin

We asked respondents their preferred services provider source in terms of origin for cybersecurity related technologies and services.

For cybersecurity technologies most prefer a global player (40%), followed by a blend of local/regional/global player (35.2%). 15.2% prefer a regional player and 5.6% a local player.

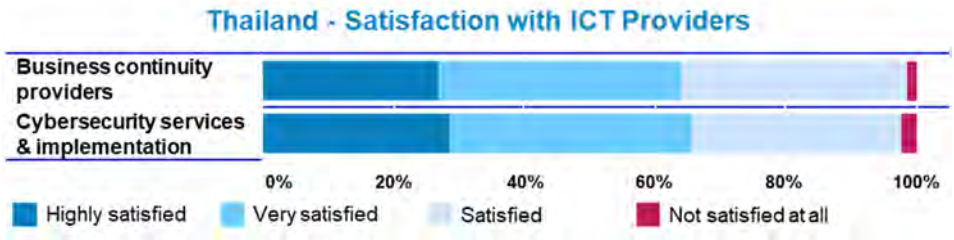
Cybersecurity Satisfaction with ICT Providers

For those respondents using service providers we asked about their level of satisfaction with the service provider. The red bars show 'not satisfied at all' and the blue bars darken as satisfaction levels increase.

36.9% of respondents are very satisfied with their business continuity providers, followed by 34.45 who are merely satisfied, and 27.0% who are highly satisfied.

For cybersecurity services and implementation, similar scores are evident. 36.9% very satisfied, 31.2% satisfied, and 29.0% highly satisfied.

Overall hardly any respondents (<2.0%) are 'not satisfied at all' across both categories.



Conclusion

Conclusion

Because cybersecurity is everywhere, it has many facets. Point solutions are still common, but most organizations with a comprehensive cybersecurity strategy have adopted a more integrated approach. There is no one size fits all solution, and every organization will need a different combination of cyber security products and services. That is all the more reason to adopt a coherent strategy rather than rely on piecemeal tactical fixes.

Cybersecurity is a broad term. It ranges from the safeguard of individual devices to the protection of the enterprise and even the nation state.

Cybersecurity is becoming very important to governments, where it is increasingly seen as an area of international conflict. Cyber warfare is a reality, with nation states 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.

It is a constant battle of changing technology. Malicious players are constantly employing new techniques and technologies and ICT faces new challenges daily.

Thai Business Leaders Responses

Cybersecurity technologies and services are used by almost all organizations in Thailand. Many different types of security initiatives have been implemented at a high level and investment plans in all areas are aggressive.

Key areas of implementation and investment include security for specific applications such as email, web, database, or enterprise wide security initiatives.

The range of services in play to support ICT organizations in their never-ending quest to secure the enterprise is large and ranges from vulnerability and penetration testing through to full-scale security implementation and managed services.

Business continuity services and infrastructure are also being treated seriously by Thai ICT decision makers.

The use of various levels of AI in support of security initiatives is high across all areas including pattern recognition of various types for identification and quarantining of threat.

Security in the cloud, poses a significant challenge for Thai ICT providers, and the criteria for selection of cloud providers now strongly reflects this need.

In general, Thai ICT decision makers are at excellent levels of awareness regarding cybersecurity threats and have implemented quite high levels of technology and invested significant shares of their ICT budget already.

However, they are not content with the status quo and continue to invest and prepare for even greater challenges.

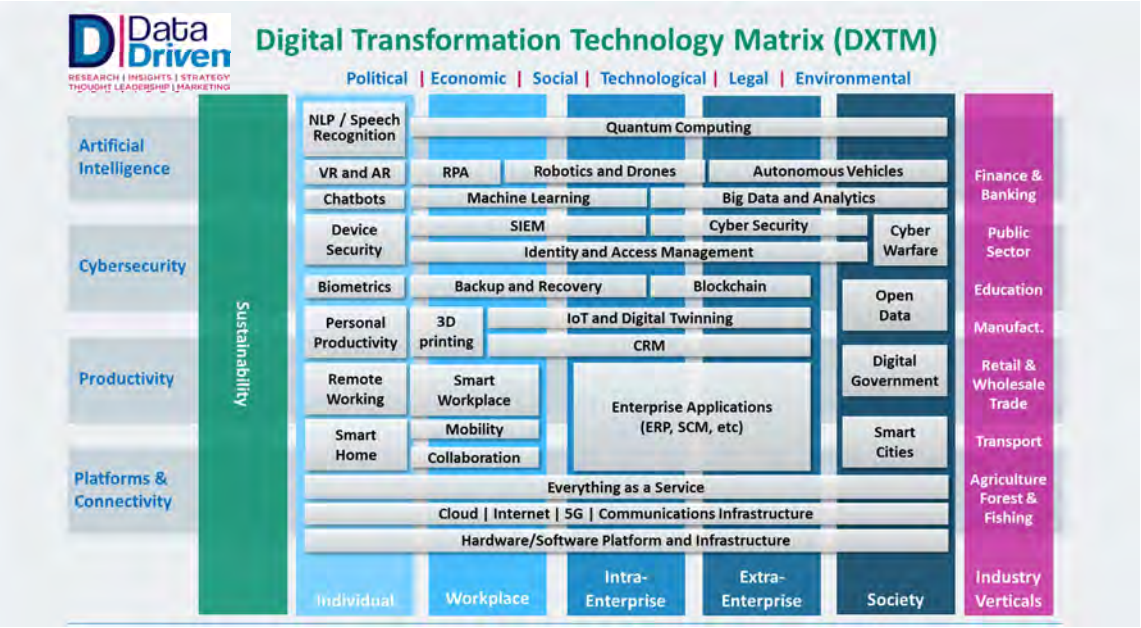
DataDriven Digital Transformation Technology Matrix (DXTM)

DataDriven Digital Transformation Technology Matrix (DXTM)

DataDriven has developed a proprietary taxonomy of technologies and trends to ensure consistency of terminology. The DataDriven 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.



Four major classes of application or technology are overlaid on these five groups. 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.

DataDriven Research Approach Based on DXTM

DataDriven Research Approach

The DataDriven Digital Transformation Technology Matrix (DXTM) enables us 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.

Demographics

Exhaustive Data Collection Process and Demographics

Thousands of potential respondents are contacted across Thailand with the aim of identifying over 100 key ICT Decision makers.

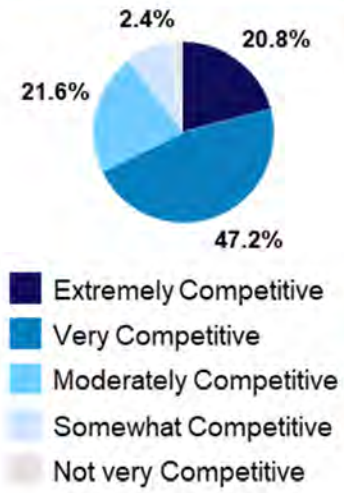
DataDriven applied 7 levels of exhaustive screening and validation questions, then conducted extensive data scrubbing and removal of non-representative data and outliers using SPSS. Visualisations were produced using Tableau and Excel.

The result is a highly qualified and reliable set of complete responses from 125 ICT decision makers.

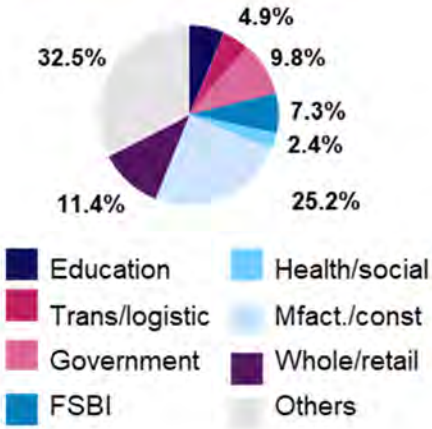
These responses have been summarised in the attached report.

Key demographic splits are shown here.

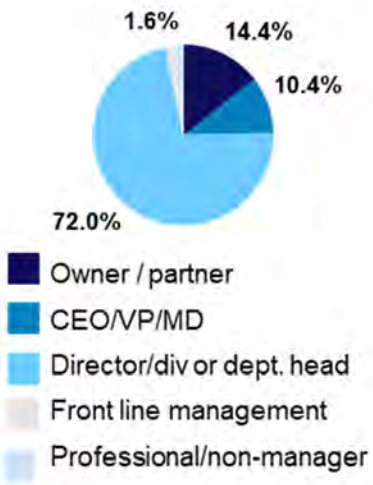
Competition Intensity



Industry Group

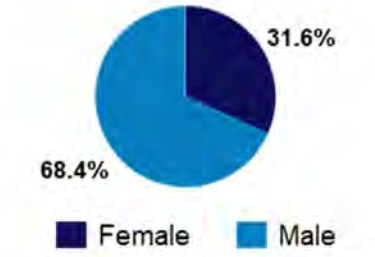


Employee Level

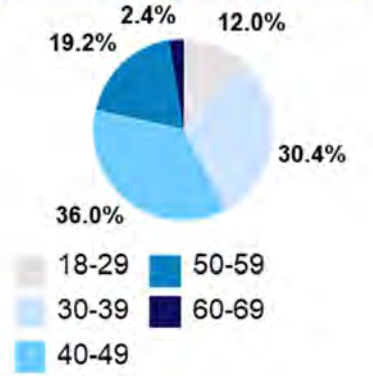


Competition Source

Gender



Age



How to Contact Us

Acknowledgement to ICT Decison Makers

DataDriven 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

About DataDriven

DataDriven 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.

DataDriven 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 DataDriven 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, DataDriven associates have supported hundreds of ICT providers and other private and public sector organizations. DataDriven has successfully executed projects globally, but has a particularly strong focus on Asia/Pacific and Japan.

Data Driven

RESEARCH | INSIGHTS | STRATEGY
THOUGHT LEADERSHIP | MARKETING

datadrivenservices.com.au
craig.baty@datadrivenservices.com.au
@CraigBaty
linkedin.com/in/craigbaty/

For further information email: Info@datadrivenservices.com.au