IDC EXECUTIVE SUMMARY

The State of IT Security in Malaysia

September 2016

By Simon Piff

Sponsored by MDEC

IT security is at the forefront of many businesses across the world and has emerged as top concern of business leaders in Malaysia in 2016. The increase in high profile hacks globally and in the Asia Pacific markets, the emergence of various types of ransom based attacks and the concern about supply chain originated attacks have made this topic a boardroom discussion. Complicating the issue is the need to transform businesses to take full advantage of the 3rd Platform technologies of cloud computing, mobile computing, Big Data and social business platforms, each of which bring with them a new set of security concerns.

Globally, IDC has observed legislation that will impact local organizations with operations in Europe and the United States, and the potential to be incorporated into local legislation is high. With fines as high as 500 million euros, the concern is very real and highly financially motivated.

As a result, organizations of all types are seeking a more robust security strategy, one that provides not only enhanced perimeter protection, but that also takes into account that the perimeter has already been breached, and permits organizations to monitor internal systems and networks equally. However, as the benchmark indicates, not many organizations have this level of maturity to date, creating an environment that is not online insecure, but one where the business is not fully trained to cope with the impact of a breach, relying instead on IT teams alone to handle this organization-wide challenge.

A mature security program is represented by a complex interplay of technology, processes, and people governed by risk management capabilities and driven by a vision that enables an organization to safely make its digital transformation. IDC has developed the IT Security MaturityScape Benchmark to help business and IT leaders understand and cope with the challenges and opportunities that digital transformation can bring to their enterprises. The current research provides objective data to help organizations identify the key capabilities that distinguish organizations whose security efforts have met or exceeded their overall expectations from their peers whose security efforts have fallen short.

Key findings of this benchmark study include:

- The majority of companies surveyed have yet to establish security capabilities and maturity at advanced levels (i.e., managed or optimized maturity) and are still at the ad hoc, opportunistic, and repeatable stages. Organizations need to integrate risk management into their decision making process and shift their focus to a distributed "tracers and tethers" model, away from a perimeter mentality.
- Organizations able to achieve greater business outcomes tend to have greater IT security maturity across all five maturity dimensions. This correlation highlights the need for organizations to become

more proactive in addressing security challenges and creating security programs that focus on the most critical aspects of the enterprise's business needs, target outcomes, and competitive environment.

In This Study

This study presents the results of IDC's 2016 Malaysia IT Security MaturityScape Benchmark Survey. It provides a comprehensive overview of IDC's IT security maturity model.

This study also presents the current state of enterprise security based on quantitative research. The results in this study will enable organizations to work with IDC to assess their security maturity level against industry benchmarks and foster the security maturity needed to compete in the new era of the 3rd Platform.

In IDC MaturityScape: IT Security (IDC #US40661915, December 2015), we identified the stages, dimensions, outcomes, and actions that organizations should consider to effectively develop IT security competency. This document enables organizations to answer the following questions:

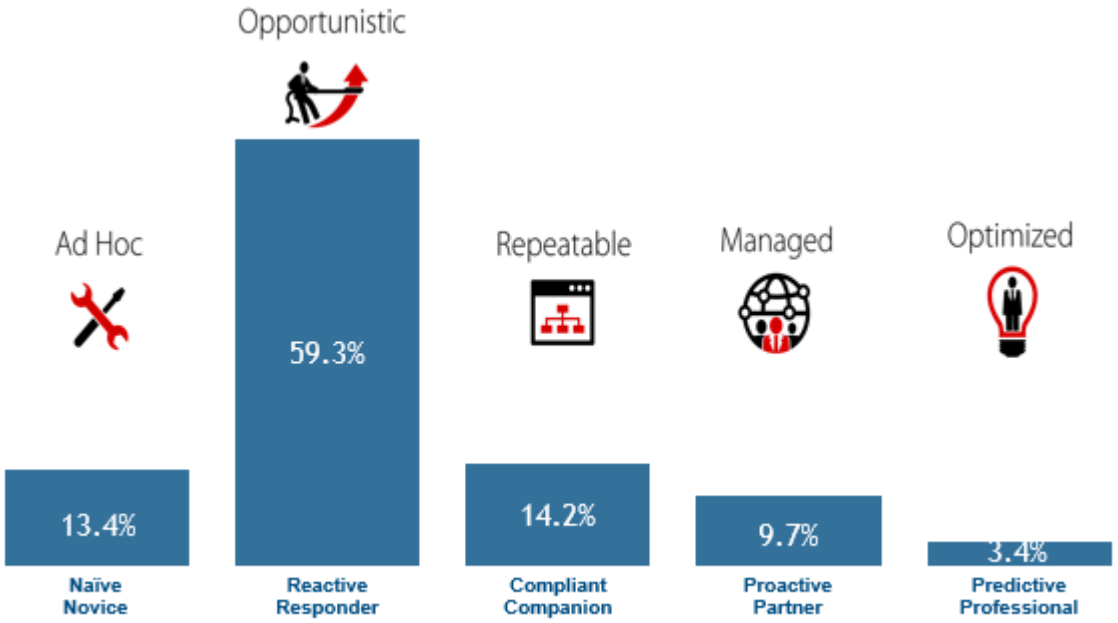
- How will security and technology risk management affect the way we do business in the era of the 3rd Platform?
- Where are we on a maturity scale for security competencies in terms of the business needs, and how does this compare with our peers?
- How should we create the framework to enable security transformation?
- What's the path to encourage and improve intra- and intergroup collaboration in promoting and encouraging a mature security program?

Figure 1 represents the maturity distribution across IDC MaturityScape stages from the simplest, unstructured ad hoc stage to the advanced, systemized optimized stage.

Please see the Appendix for detailed methodology, market definition and scoring criteria.

Figure 1

IT Security Maturity Distribution Across Stages



n = 106

Source: IDC's Malaysia IT Security MaturityScape Survey 2016

Situation Overview

IT Security (ITSec) is becoming a far more essential component of the overall IT architecture for all types of organizations, be they commercial, charitable or government. The implications of data loss or technological breaches have financial, reputational and national security impact that is growing in importance and interest with every passing year. Whilst implanting a robust and mature ITSec process will not guarantee the security of your organization or data, it will provide the organization with world class ability to react in a timely manner to address threats and breaches, hopefully before any data is lost or systems compromised.

Digital transformation requires technology risk management. It forces enterprises to consider its practices and control implementations in newer, uncommon ways to simultaneously address concerns and drive the business forward, all under the possibility of being thrust in the public eye by experiencing a threat or breach that may or may not have been preventable.

Leaders in digital transformation must also be leaders in technology risk management, as they have the most to lose, both economically and reputation wise. This IDC IT Security MaturityScape provides a tool to enable organizations to:

- Assess their security capabilities and stage of maturity.
- Understand the challenges and opportunities.
- Identify areas necessary for improvements.

- Create the road map and the framework to enable their security transformation.

Many large organizations have had a defined plan and a committed budget to strengthen their company's security program. However, the plethora of technology choices, the range of security technology and risk management skills, and the amount of hype have all made it difficult for many organizations to prioritize resource allocations toward their security initiatives and coordinate all the moving parts to successfully implement a cohesive security strategy. IDC believes that organizations need to have a more proactive and predictive approach to their security objectives.

IDC's IT Security MaturityScape enables businesses to assess their organizations' competencies to foster and leverage the security maturity with respect to the five key dimensions: vision, risk management, people, process, and security technologies. Each dimension is targeted at a key aspect of IT security mastery and can be assessed as an independent measure as well as in conjunction with other dimensions.

Stages of IDC's IT Security MaturityScape

IDC's IT Security MaturityScape consists of five stages: ad hoc, opportunistic, repeatable, managed, and optimized. For each stage, the IDC IT Security MaturityScape Benchmark addresses how capabilities for a particular dimension need to change to foster the security maturity needed to compete in the new era of digital transformation. The key characteristics of the five maturity stages are:

Ad hoc — naïve novice: Employ basic operational security measures and act on security needs as they arise.

Opportunistic — reactive responder: Full-time staff address most significant security requirements but look to external sources to provide guidance in compliance-oriented program.

Repeatable — compliant companion: Solid security program and control framework address all regulatory needs and internal risk assessments.

Managed — proactive partner: Robust security program includes strong compliance and early exploration of the cost-effectiveness of solutions.

Optimized — predictive professional: Risk is recognized as an element of overall business value proposition for technology, and the security strategy approach seeks most efficient and effective ways to manage enterprise security.

Survey Findings: Maturity Distribution Across Stages

Refer back to Figure 1 to see the aggregated maturity distribution across all five IT security maturity dimensions. The highlights of IDC's 2016 IT Security MaturityScape Benchmark Survey are as follows:

- A small but noticeable percentage of respondents (13.4%) of organizations are still at the least mature, ad hoc, stage. These organizations lack basic security strategy and management support. Security receives attention only when the issue arises out of their business interests such as doing business with partners that require security information, entering into a regulatory environment, or actually experiencing a breach. Based on our study, organizations at this stage are generally smaller, and it often takes a significant breach to aspire to move to higher maturity stages.

- A majority (59.3 %) of respondents indicated that their organizations are at the opportunistic stage. These organizations have taken guidance and addressed security needs to provide protection for their environments, some at a heavy expense. However, organizations at this stage are often inefficient and ultimately designed only to meet compliance and regulation requirements. They have not leveraged risk management to improve IT productivity or create significant value for the organization. IDC believes that these organizations need to move to the managed or optimized stage to enable digital transformation and service innovation.

- Only 14.2% of the respondents fell into the repeatable stage which is not too surprising. Defined as the "compliant companion", organizations in this stage are characterized as being able to respond to compliance requests and are the regulators' dream. They buy into the need for security and, guided by the advice of auditors, invest heavily in their security and compliance program with the goal of providing the best protection for their environments. IDC believes that maturing of legislation in the areas of privacy and data security will lead to an increase in this stage in the coming future.

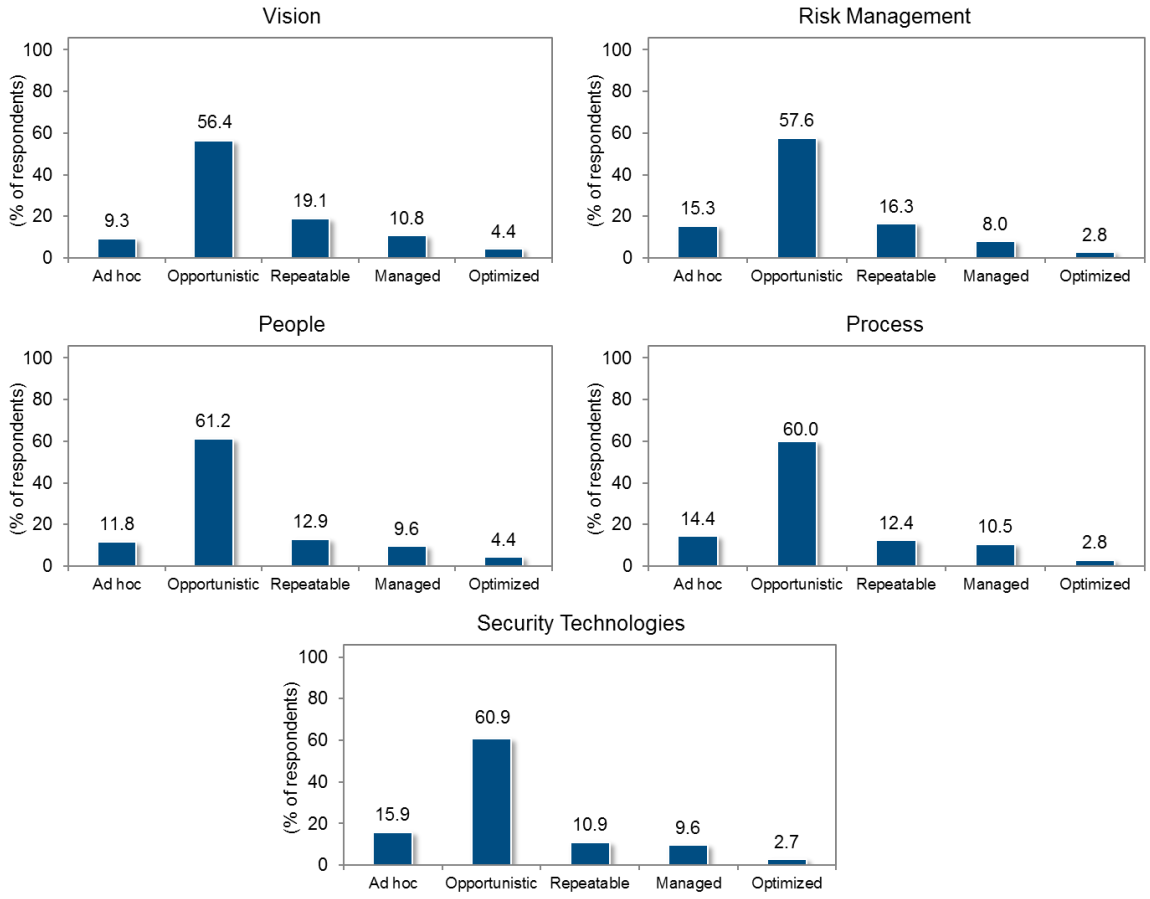
- Less than one-fifth of respondents (9.7%) are at the managed stage where their organizations focus on the cost-effectiveness of their security programs and work to become more proactive in evaluating security controls. These organizations have developed a security strategy based on their business needs and value proposition of their security programs. IDC believes that these organizations are starting to enjoy competitive advantages brought by deploying mature risk management and more progressive technology initiatives.

- There is a small percentage of respondents (3.4%) that are at the optimized stage. Organizations at this stage have already integrated the risk management approach into their business management. These organizations recognize the nature of uncertainty and proactively employ security tools and solutions to predict and manage risks. This creates a resilient environment for these organizations to avoid, respond to, and recover from potential breaches. IDC expects that, in the next three years, many enterprise/large organizations will commit budgets and resources to strengthen their organizations' security strategy to move to the optimized stage.

These results provide a consolidated current view of the overall security maturity among Malaysian organizations. A successful security program depends on a multipronged approach guided by a strategy that focus on not just security technologies but also identity, leadership, and processes. To help organizations understand the underlying strengths and weaknesses of their security programs and compare them with their peers, we also measured maturity across the five key dimensions of the IT Security MaturityScape (see Figure 2).

Figure 2

IT Security Individual Dimensions Maturity Distribution Dashboard



n = 106

Source: IDC's Malaysia IT Security MaturityScape Survey 2016

Dimensions of IDC's IT Security MaturityScape

To view the opportunities and challenges more clearly as IT moves through the various stages of IT security maturity, organizations need to understand the five critical dimensions. Note that the dimensions of IDC's IT Security MaturityScape and their characteristics at each stage of maturity are highlighted in IDC MaturityScape: IT Security (IDC #US40661915, December 2015). The details of the dimensions are as follows:

- **Vision** evaluates business objectives, security objectives, financial and economic needs, and regulatory oversight.
- **Risk management** evaluates the risk approach, methodologies, external relationships, and control environment of an organization.
- **People** evaluates the executive leadership, organizational culture, security executives (CISO), and security worksourcing aspects of an organization.

- **Process** evaluates the processes surrounding trust management, identity management, vulnerability management, and threat management in an organization.
- **Security technologies** evaluates the identity management, vulnerability management, threat management, and trust management tools and technologies in use at an organization.

Improving IT Security Maturity: Survivors and Thrivers

The IDC MaturityScape framework is structured in part to not only identify what a particular level of maturity requires but also enable leaders to assess just how much maturity they need at any given point in time.

As part of IDC's IT Security MaturityScape Benchmark Survey, we asked organizations to self-assess their approach to vision, risk management, people, process, and security technologies in the context of their overall ability to leverage their IT security programs (see Figure 3). Based on this result, we segmented organizations into two categories:

- Survivors: Organizations that have basic and/or formal security programs but ultimately don't consider security valuable in a strategic business sense
- Thrivers: Organizations that have advanced capabilities and are constantly seeking the maximum "risk reduced per unit cost"

Survey Findings: Comparison of Survivors and Thrivers

Figure 3

IT Security Dimensions Dashboard: Comparison of Survivors and Thrivers

n = 106

Source: IDC's Malaysia IT Security MaturityScape Survey 2016

Essential Guidance

Having an effective, mature security program is a precursor for creating healthy and innovative organizations in the 3rd Platform environment. For IT executives in world-class enterprises, knowing their security maturity level is essential to enable them to understand what their current security program is capable of delivering, to grasp what maturity level is required to achieve target business objectives, and to identify the next steps to closing that maturity gap. Although many factors can affect the efficiency and effectiveness of an organization's path toward greater IT security maturity, we found that the factors described in the sections that follow have the greatest impact on the five IT Security MaturityScape dimensions.

Table 1

Top Traits of Thrivers' IT Security

Maturity Dimension	Trait
Vision	Technology-related risk assessments have been factored into the management program, and there is protection against advanced threats.
Risk management	A cost-utility analysis is conducted to seek optimal "risk reduced per unit cost" for IT security projects.
People	There are collaboration processes among staff and security executives to assess technology risks and control costs as part of IT decision making.
Process	Risk management and security operations within the organization are defined, measured, and managed based on clearly understood metrics.
Security technologies	Defined tools and solutions are used for identity management, vulnerability management, threat management, and thrust management.

n = 106

Source: IDC's Malaysia IT Security MaturityScape Survey 2016

Based on the findings in this study, we suggest that organizations should have a balanced approach to investing across all five IT security maturity dimensions. The following sections provide insight into increasing maturity levels in each of the five dimensions of IDC's IT Security MaturityScape.

Vision

- Provides the context for organizations.
- Incorporates sub-dimensions for business objectives, security objectives, financial and economic needs, and regulatory oversight into a cohesive and strategic approach for technology risk management in the enterprise.
- Organizations progress through the maturity stages by increasing the integration of security and risk discussions with business units and across the enterprise while simultaneously looking for ways to reduce risk for the lowest cost.

Risk Management

- Takes the strategic business objectives of the vision dimension and builds out the security program requirements in a more specific way by addressing sub-dimensions for the risk approach, methodologies and measurement, external relationships, and control environment.
- Organizations progress through the maturity stages by increasingly assessing evidence and outcomes associated with risky activities and developing a more scientific feedback loop to build the security program.

People

- Involves the roles of executive leadership and the overall organizational culture in a maturity model
- Builds out stages of maturity for security executives and security worksourcing for the custodians and administrators of the program itself.
- Organizations progress through the maturity stages by incorporating executive opinions, enterprise user behaviors, and security professional activities into a robust program of awareness, inclusion, and decision making.

Process

- Describes the activities that an enterprise employs to manage risk in an operational environment.
- Builds out the stages for four sub-dimensions — trust, identity, vulnerability, and threat management.
- Organizations progress through the maturity stages by increasing the scope and automation of the traditional processes in place, constantly looking for ways to reduce risk with the lowest cost.

Security Technologies

- Includes how various security programs leverage technology for protecting resources throughout the technical architecture for trust, identity, vulnerability, and threat management.
- Organizations progress through the maturity stages by creating a digital security technical architecture that matches the dynamic, distributed architectures of today's IT environments.

Learn More

Methodology

The results in this study are based on IDC's 2016 Malaysia IT Security MaturityScape Benchmark Survey of 100 organizations in Malaysia, conducted in July/August 2016. The survey, executed via phone, was based on a structured questionnaire of 32 questions. These survey questions were focused on the five dimensions of IDC's IT Security MaturityScape. For each dimension, we created a set of questions to assess the level of capability/maturity for the dimension.

Note: All numbers in this document may not be exact due to rounding.

Survey Respondent Segmentation

The survey respondents were segmented as follows:

- All of the respondents were from Malaysia
- 21.9% of the respondents were from organizations with 5,000+ employees, and the rest (78.1%) of the respondents were from organizations with 1,000-4,999 or less employees.
- The respondents were from 16 different industries — 5.9% of them were in the professional services industry (legal, accounting, engineering, etc.), and 13.9% of the respondents were in transportation services.
- All of the respondents had the title of manager of IT or higher — 16% of them were CIO or vice president of IT in the organization.