IDC
Analyze the Future

IDC EVENT PROCEEDINGS

Security by Design: Preparing for the Inevitable

November 2016

By Linda Chua and Simon Piff

Sponsored by MDEC

*Malaysia Digital Economy Corporation (MDEC), in collaboration with IDC, launched the **CIO Survival Guide** series in 2013. As part of its continued effort to support the growth of Malaysian businesses, MDEC is focused on helping CIOs and senior IT executives cope with the rapidly changing technological landscape by equipping them with information and resources to make well-informed decisions for their organizations. The fourth workshop in the series, themed "Security by Design — Preparing for the Inevitable", was held at the Le Méridien Hotel on September 27, 2016, in Kuala Lumpur. The one-day event focused on the struggles of CIOs in delivering returns of IT security investments against the backdrop of digital disruption. More than 80 CIOs and senior IT executives attended the workshop facilitated by Simon Piff, Associate Vice President of Enterprise Infrastructure research, IDC Asia/Pacific.*

Driving Malaysia's Digital Ambitions

As technologies change, so does the role of CIOs. In today's digital era, CIOs have a mandate to drive digital transformation (DX) in their organization, and many executives still do not fully understand what is required. Citing global projections of the economic impact of DX, Dato' Ng Wan Peng, chief operating officer, MDEC, noted a 0.5% increase in per capita GDP for a 10% increase in digitalization. Highly digitalized sectors can also expect a four-fold productivity increase compared to those that have not jumped on the DX bandwagon.

MDEC will continue to push industries to adopt emerging technologies that enable digital innovation and the Internet economy. The positive impact of DX on the Malaysian economy is expected to continue and raise the country's gross national income, business productivity, and standards of living. According to MDEC, the ICT industry and its sub-sectors contributed 17% to Malaysia's GDP in 2014 while traditional economic sectors contributed 83%. The ICT sub-sectors included are services, manufacturing, content, ecommerce, and trade. If the remaining traditional economic sectors were included, a healthier growth contribution of 23% to the nation's GDP is possible.

MDEC will continue to champion the digital economy to boost the country's economic growth. It also intends to widen its focus beyond developing the supply side of the ICT industry to include the digitalization of traditional ecommerce sectors that need a boost.

The main barriers to the adoption of DX in Malaysia are low awareness, lack of DX talent, skills and capabilities, as well as a lack of drive from management around digital strategies and capabilities. Cost concerns, building a business case and quantifying the return on investment (ROI), and integration of DX with core business strategies and operations are also focus areas.

MDEC also recognizes the need to build a strong ecosystem around cybersecurity in Malaysia, and welcomes collaboration with all stakeholders, including regulators, vendors and users, to identify areas

such as policy regulations, compliance requirements, and security solutions required to meet the needs of the new marketplace.

MDEC is working to:

- Create a security aware culture and ownership for driving business value
- Put in place a process framework to measure the impact on digital assets
- Identify the architectural support needed for cybersecurity

Dato' Ng emphasized that Malaysia organizations should jointly explore how they can tackle cybersecurity issues, develop security capabilities, and deploy digital platforms and systems while safeguarding against potential cyberthreats.

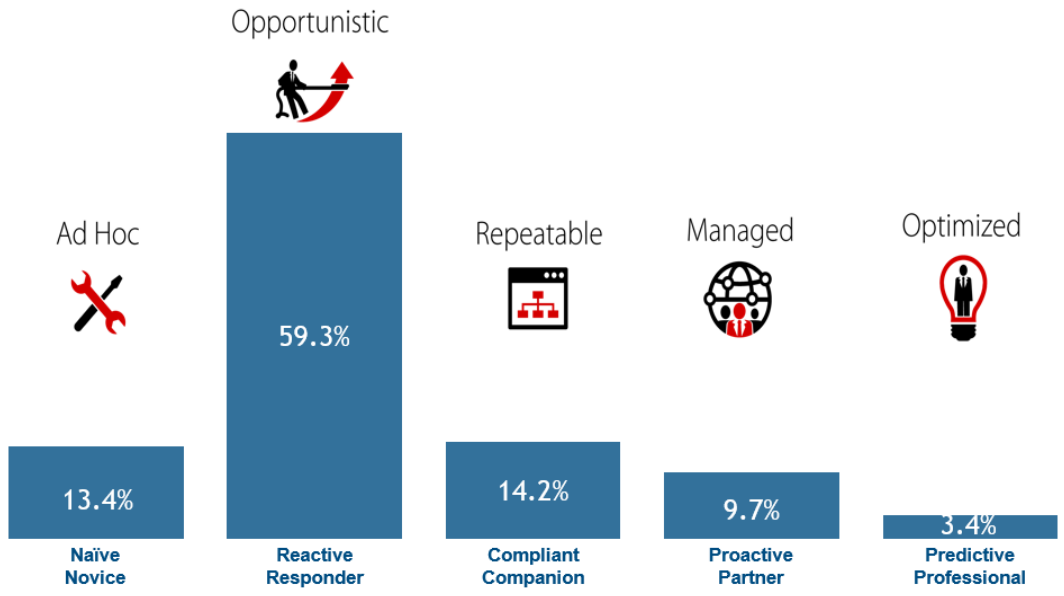
The CIO Imperative: Preparing for the Changing Cyberthreat Landscape

Today's increasingly sophisticated threat landscape is shifting in favor of the bad guys. Cyberattackers are well-funded, use cloud, automation and big data tools to seek out and identify soft targets that they can rapidly monetize through different approaches. IT organizations, however, are under-funded, rarely have the executive support and processes in place, and are supposed to deliver a secure environment in a world in which 100% security can never be achieved. Since it is inevitable that all organizations will experience some form of data breach, loss or denial of service or access, at some point in the future, how prepared are today's organizations for cyberthreats?

Almost three-quarters (72%) of the 106 Malaysian organizations that participated in IDC's IT Security MaturityScape survey are still in the early stages of IT security maturity (see Figure 1).

Figure 1

IT Security Maturity Distribution Across 5 Stages



N=106

Source: IDC's IT Security MaturityScape Benchmark Survey 2016, sponsored by MDEC

Organizations in the Ad Hoc and Opportunistic stages largely operate in a reactive mode. Those in stage 1, the least mature, employ basic operational security measures and act on security needs as they arise. “Reactive responders” or stage 2 organizations have full-time staff overseeing most significant security requirements but look at external sources to provide guidance in compliance-oriented programs. More than half (59.3 %) of the entire survey pool are at this stage; they have taken guidance and addressed security needs to provide protection for their environments, some at a heavy expense. However, these organizations 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 stages to enable DX and service innovation.

So how best can CIOs prepare their teams, the executive, and the border organization to respond and minimize the risks? To answer this question, attendees participated in a workshop and were broken into four teams. They were asked to define the plan of action in the event of a hacking incident. The CIOs’ biggest concern was disruption to the business, and they agreed that having a cybersecurity framework was critical for business success.

A cybersecurity framework should:

- Cover people, process and technology as well as consider both internal and external issues.
- Take into account the type of attack that is taking place and then provide documented guidance on what needs to happen.
- Include guidance that covers internal and external IT help (including service providers) as well as the level of engagement needed with the business.

Attendees identified several issues and takeaways as actions for both the IT team and the business as a whole to restore the business to its normal operations following the hacking incident.

The first was to **engage more outsourcing services in areas such as security monitoring** that are not part of their core specialties. For example, round-the-clock surveillance is largely employed in the banking and financial services sector.

One concern, however, was the potential high cost of outsourcing cybersecurity monitoring in Malaysia, to which MDEC suggested **multiple tiers of service delivery** that could encompass a broader range of price points. The **use of alerts and trigger firewalls** was also highlighted as a way to manage cost.

Attendees raised a second point around staffing resources. Not only do organizations find this an ongoing challenge, they find it equally difficult to justify the cost. As IT teams are generally small, the role of security falls on everyone, with no opportunity to have dedicated headcount. This makes the “ideal scenario” of having dedicated security resources almost impossible for most Malaysian organizations.

Given that cybersecurity threats know no boundaries, attendees highlighted **the need for more laws, such as a cybersecurity disclosure law**, to be introduced on top of the Personal Data Protection Act that is already in place.

Another related cost concern was around the setting up of datacenters in Malaysia, which attendees noted as “high” due to the high telecom and fibre infrastructure costs. Majority of the organizations prefer to work with global vendors instead of local vendors, and are comfortable having datacenters or their data being in Singapore, regardless of the impact to the local ICT economy.

Conclusion

Digital transformation requires technology risk management, and organizations need to understand their security posture, develop a cybersecurity framework, and prioritize internal security resources.

The workshop discussion throws the spotlight on the business realities of cost and resource challenges facing Malaysia businesses, and make many of the global benchmarks challenging to attain. Whilst security remains a high concern, the pragmatism that is required to manage within these aforementioned confines will likely result in little change to the current status quo.

What will be needed are ongoing efforts that explore how Malaysian organizations can collaborate to tackle cybersecurity issues, develop better security capabilities, and deploy digital platforms which, at the same time, safeguard them from rising cyber threats.
