Managing and Understanding Cyber Risk Exposure in Asia Pacific

An IDC InfoBrief | May 2018

IDC ANALYZE THE FUTURE

Sponsored by tenable

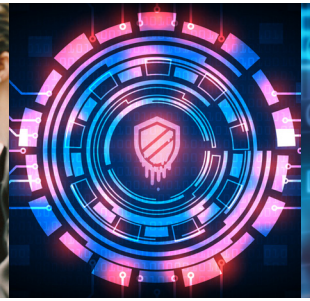
Digital transformation drives IT investment in Asia Pacific (AP), but cybersecurity struggles to maintain pace

Cybersecurity conversations with the board have to be "risk-based" conversations, with clear metrics on the perceived exposure, a prioritized plan on how to reduce it and a value-based conversation around "risk reduced for dollar spent."

This is not the case for most organizations across the region as they are mostly unaware of the exposure due to time and cost pressures across a range of other responsibilities.

Security leads need to step out from the tactical shadows, to emerge as strategic, risk-aware thought leaders who can contextualize risk in business terms for their CEO and boards.

This requires a change in the approaches taken and the conversations currently being had.



Lack of awareness of the tools that can address the challenges of securing vulnerabilities created by evolving IT ecosystems.

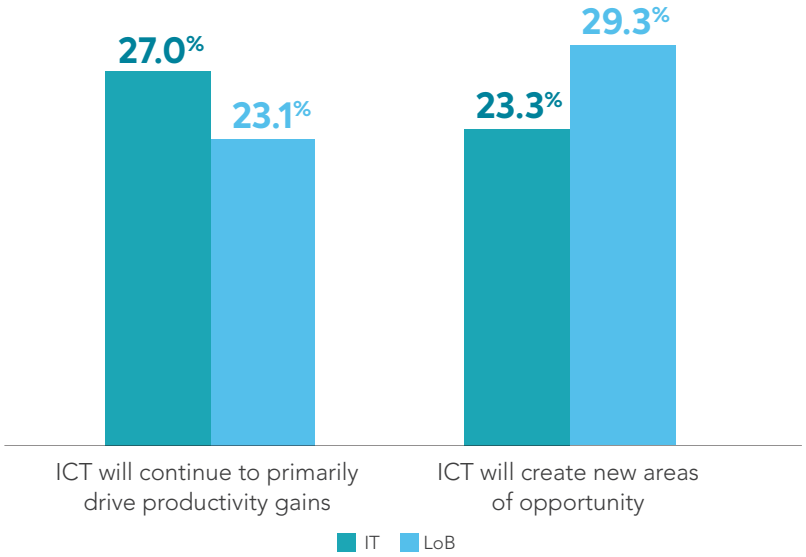
In spite of Risk Management being #5 in the Top 5 most important technologies to enhance competitive position[1], IDC has discovered that Risk Management skills are lacking across the region.[2]

IDC ANALYZE THE FUTURE

[1] IDC Asia/Pacific C-Suite Barometer 2017
[2] IDC MaturityScape Benchmark: IT Security in Asia/Pacific (Excluding Japan), 2017

The IT/LoB communications gap in AP

What role does ICT play in your organization?



Digital transformation (DX) is driving new business opportunities, for those able to leverage the underlying technologies securely.

Line of business (LOB) has higher expectations of DX-era innovation from IT than IT leaders themselves express.

The IT security conversation is rarely delivered well nor well-received by the business due to a communications gap between the C-suite and highest levels of IT management.

This needs to change if business is to securely leverage the technologies needed to compete in the DX economy.

Security lacks a strategic conversation in AP

Attitudes to IT security

31.2% CIO/CISO updates the board regularly

24.1% CEO has made this a key KPI for its management team

19.5% All employees have to be security certified annually

37.7% Cybersecurity compliance is required

43.1% Cybersecurity is a key IT initiative

19% No broad base strategy or governance framework

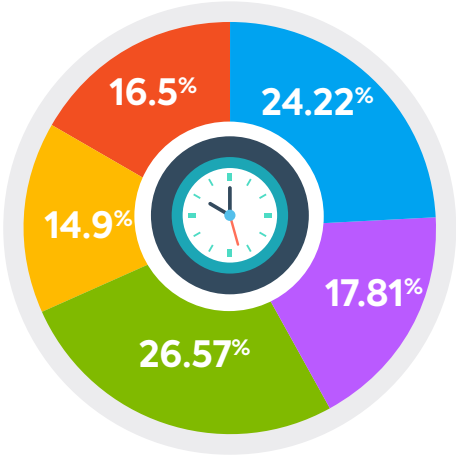
Too few organizations make IT security, and the associated risk exposure, a strategic priority; only 31.2% of IT leaders update the board.

Part of the challenge is in the provision of data that links business imperatives to IT security in a language the board understands, permitting it to make quantifiable decisions on the issues at hand.

Understanding the nature and criticality of where organizations are exposed is the foundation of a more strategic cybersecurity conversation with business decision-makers.

IDC ANALYZE THE FUTURE

Time allocation of CIO



Breadth of workload contributes to the inability of IT leadership to craft this C-level communications strategy.

Governance

Innovation

IT operations

Vendor/solution sourcing/project management office (PMO)

IT service delivery management

IDC Asia/Pacific C-Suite Barometer 2017

AP lacks IT security maturity

Risk Management

43.2% Ad Hoc

40.3% Opportunistic

10.2% Repeatable

5.5% Managed

0.8% Optimized

In *IDC MaturityScape Benchmark: IT Security in Asia/Pacific (Excluding Japan), 2017*, almost half of the region is still in Ad Hoc stage (43.2%). Security receives attention on a need-to-have basis 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.

Security Technologies

46.9% Ad Hoc

39.8% Opportunistic

7.1% Repeatable

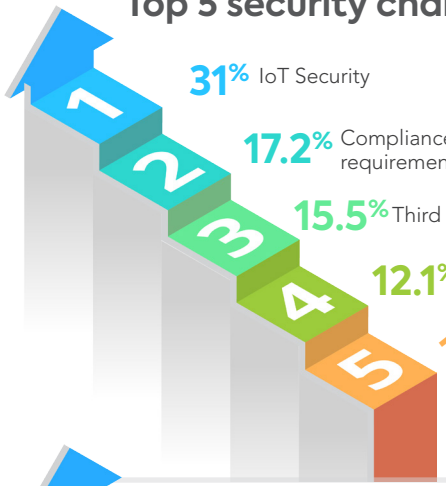
5.6% Managed

0.6% Optimized

Risk management capabilities and security technologies dimensions are two areas where organizations could improve their overall security posture. Having better risk management processes, and moving from purely defensive to detection and remediation technologies would enhance the capabilities of many organisations.

Top of CISOs' minds – new threats and ongoing risk management

Top 5 security challenges for the CISO



1. 31% IoT Security
2. 17.2% Compliance and audit requirements
3. 15.5% Third party vendor management
4. 12.1% Managing expectaions of the CEO/Board of Directors
5. 12.1% Employee IT security awareness

Top 5 concerns of Chief Information Security Officers (CISOs) in Asia Pacific reveal a surprising admission that the concern of new technologies, compliance and 3rd party vendor management are considered more important than managing board expectations.

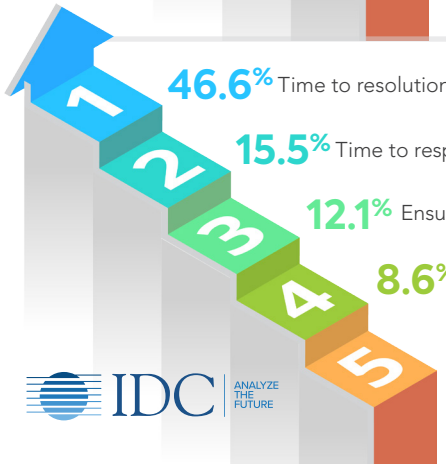
Considering where the funding decisions are being made, this reveals that perhaps CISOs are unable to surpass the day-to-day execution challenges to understand the strategic role they play in mitigating areas of IT vulnerability in their organization.

That something as tactical as Internet of Things (IoT) security is highlighted indicates that the role is still at a nascent, and largely tactical stage in the Asia Pacific markets and the shift towards strategic alignment with the Risk Committees and the board is still unrealized.

Understanding risk exposure, and moving towards benchmarking this against industry peers should be a top priority for security leads.

Key Performance Indicators (KPIs) around reducing risk/dollar spent should become CISO KPIs.

Top 5 CISO KPIs



1. 46.6% Time to resolution
2. 15.5% Time to respond
3. 12.1% Ensuring 100% compliance
4. 8.6% Improving time to identify a malicious event
5. 6.9% Enabling secure business innovation

CISOs KPIs are also not aligned to the needs of the business

Lacking is a focus on identifying potential exposure

If the issue cannot be seen, it can never be resolved

IDC ANALYZE THE FUTURE

IDC Asia/Pacific C-Suite Barometer 2017

Addressing the challenge

New business models in AP will introduce more risk, therefore new tools and processes must be adopted if cybersecurity is going to be able to keep up.

IDC Predictions

25%

By 2020, 25% of spending will be on vendors who provide a tightly integrated platform approach to security.

50%

By 2020, 50% of security telemetry will be made more useful via the use of machine learning and cognitive software, which will ingest and curate it into actionable and intelligent data at record speed.

IT security systems have been built up over a period of time with many discrete tools, resulting in a complex array of solutions that do not interconnect nor integrate, and thereby increasing the potential for exposure to risk. This will have to change in the near future, and CIOs are advised to start this rationalization process early, before Chief Financial Officer (CFO) become engaged and drive this home faster, and perhaps with less diligence.

Artificial intelligence is being built into security solutions to aid in managing and identifying the risks and potential exposure organizations have to cyber threats.

These two trends will permit CIOs to refine the incoming data for security issues and begin to create the base data-sets from which a robust risk management narrative can be built, which is the missing link today between IT security communications with the CEO and the board.

IDC ANALYZE THE FUTURE

What needs to happen

CISOs need to be able to communicate IT security issues in business terms to the CEO and the board in order to help remediate the issues they face around funding and resourcing for cybersecurity.

This conversation needs to be a risk-based conversation, highlighting the most critical risks an organization faces at any point in time. It needs to be based on understanding their exposure, prioritizing the risk based on business metrics, and providing a clear plan on how these risks will be mitigated over time by the strategy proposed.

Areas to be addressed would include:

- **Where are our vulnerabilities?**
- **How do we incorporate risk metrics into our priorities?**
- **How well are we reducing exposure over time?**

Benchmarking this reduced-risk against peers is a goal that should be in the sights of CISOs.

IDC ANALYZE THE FUTURE

Tenable vision: Solving the cyber exposure gap

- Cyber Exposure is a new approach to manage and measure the modern attack surface to accurately understand and reduce your cyber risk
- Entails a full lifecycle (Discover, Assess, Analyze, Fix and Measure)
- Tenable.io Lumin is the first cyber exposure platform that empowers CISOs to confidently visualize, analyze and measure cyber risk
- Leverage context and intelligence to prioritize and remediate more effectively, based on risks. Measure risk reduction and compare performance to industry peers (i.e., benchmarking)
- Make better strategic decisions - manage cyber risks objectively, similar to other business risks
- Elevate the conversation – CISOs become risk strategists and advisors

IDC | ANALYZE THE FUTURE

Sponsored by tenable™