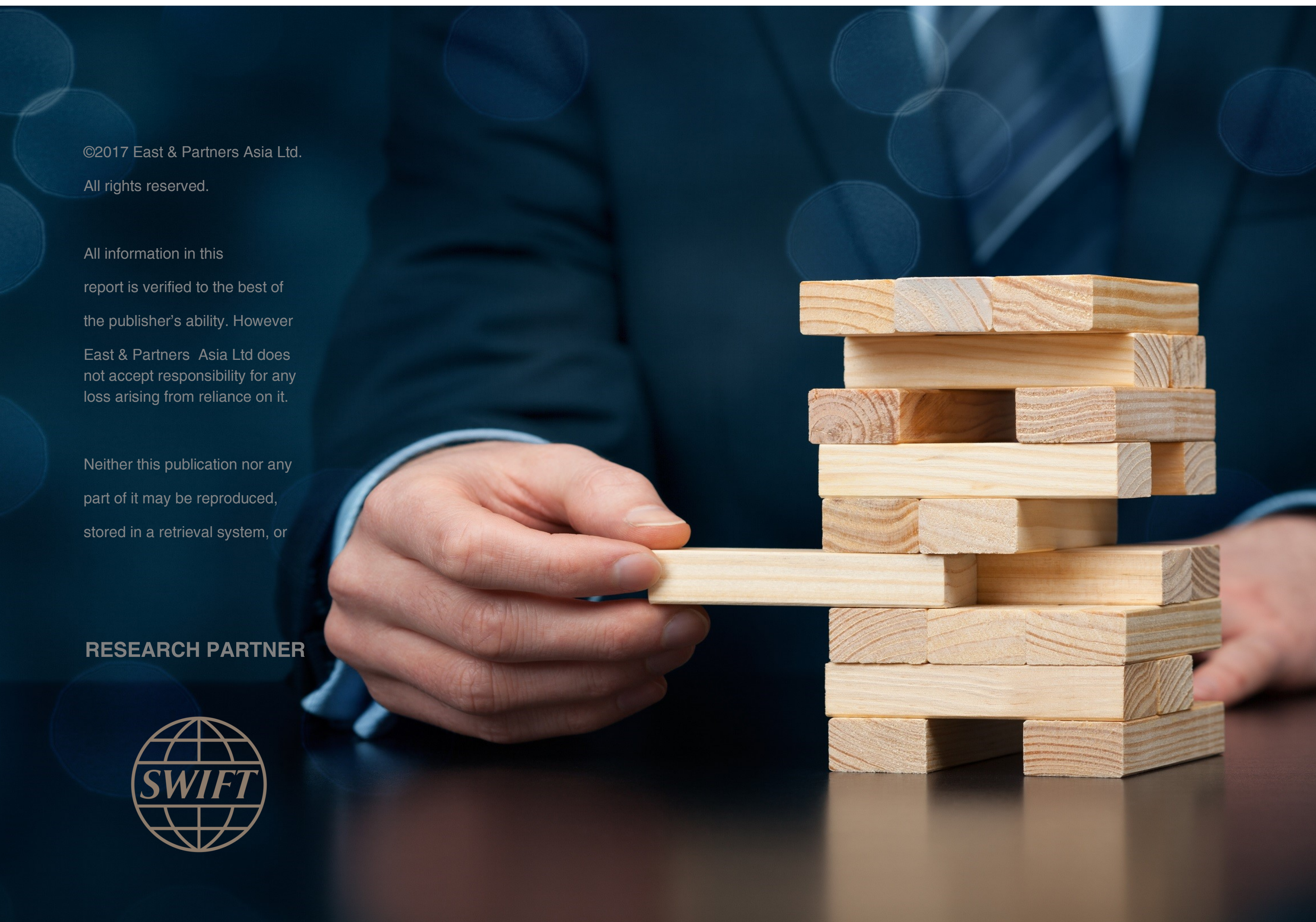
east&partners asia

RISK AND COMPLIANCE INDEX:

Vulnerabilities and Priorities for Corporates in Asia Pacific



RESEARCH PARTNER

SWIFT

Executive Summary

The pace and complexity of regulatory change in financial services and corporate governance continue to grow following a range of global scandals that have come to light, driving an escalating focus on how corporates in Asia are managing these risk issues. With stakeholders' expectations rising, coupled with stricter enforcement actions and higher fines, not to mention reputational risk, it is unsurprising that corporates are becoming more focused on managing risk and compliance effectively.

SWIFT has commissioned East & Partners Asia (E&P) to conduct the Asia Pacific Corporate Risk and Compliance Index research to gain further insights into prevailing corporate risk management and compliance practices, cyber threat readiness, external vendor engagement and future directions in risk management. This study, based on direct interview with 915 of Asia's Top 1,000 revenue ranked corporates across 10 major economies in Asia Pacific, reveals that corporates in region are clearly alert to the risks of poor compliance and risk management, including cybersecurity behaviour.

In general, corporate risk and compliance functions in Asia Pacific are still in their infancy as a majority of corporates do not have a dedicated Chief Risk Officer (CRO). Key gaps identified in the risk and compliance governance include the low, although growing, level of cyber awareness at management level and a relative lack of standardised internal procedures to manage newly identified risks.

A significant difference in view on responsibility concerning compliance between key markets in the Asia Pacific region is also evident. Moving forward, corporates plan to improve their existing strategy by integrating risk and compliance processes into the business more completely through engagement with quality external advisors.

In these pages, you will find key takeaways of the research on page 2 followed by the main risk and compliance concerns for corporates in Asia Pacific. Subsequent sections will dive deeper into the top two concerns – cybersecurity and regulatory compliance. This is followed by risk management benchmarks and calls to action. Research methodology and interviewee profiles are appended at the end for further reference.

SWIFT as the world's leading provider of secure, standardised and seamless financial communication is uniquely positioned to support financial institutions and corporates to establish risk and compliance controls. By highlighting the dominant concerns in this space and current benchmarks in risk management, corporates can use the information provided to develop a clear next step – to move beyond a reactive, cost-driven approach to a proactive, overall compliance with very clear business and competitive benefits for investment.

I. The big risk and compliance concerns for Asia Pacific corporates

II. Cyber threats coming – are you ready!

III. Your regulatory compliance behaviour

IV. Risk management benchmarks - call for improvement

RESEARCH PARTNER

Key Takeaways

East & Partners spoke on behalf of SWIFT with 915 CFOs, Treasurers and CROs across 10 countries in Asia Pacific for the Corporate Risk & Compliance Index. The key findings, examined more closely in the body of this paper, include the following:

Compliance policy is driven primarily by external penalty avoidance and reputational factors

Half of Asia Pacific corporates view banks as having primary responsibility for compliance to the exclusion of the corporate entity.

Over a third of corporates who experience cyber breaches report monetary losses while nearly 20 percent also highlight a breach of client data.

Integrating risk and compliance into the business more fully, getting on the front foot and improving external risk management are key areas of focus for current risk and compliance management processes.

Lack of standardised internal procedures to manage newly identified risks across all countries, but particularly in developing markets, corresponds to high data and monetary loss incidences.

When turning to external providers to supplement internal risk management, Asia Pacific corporates favour legal advisors, technology vendors and specialist consultant providers over banks.

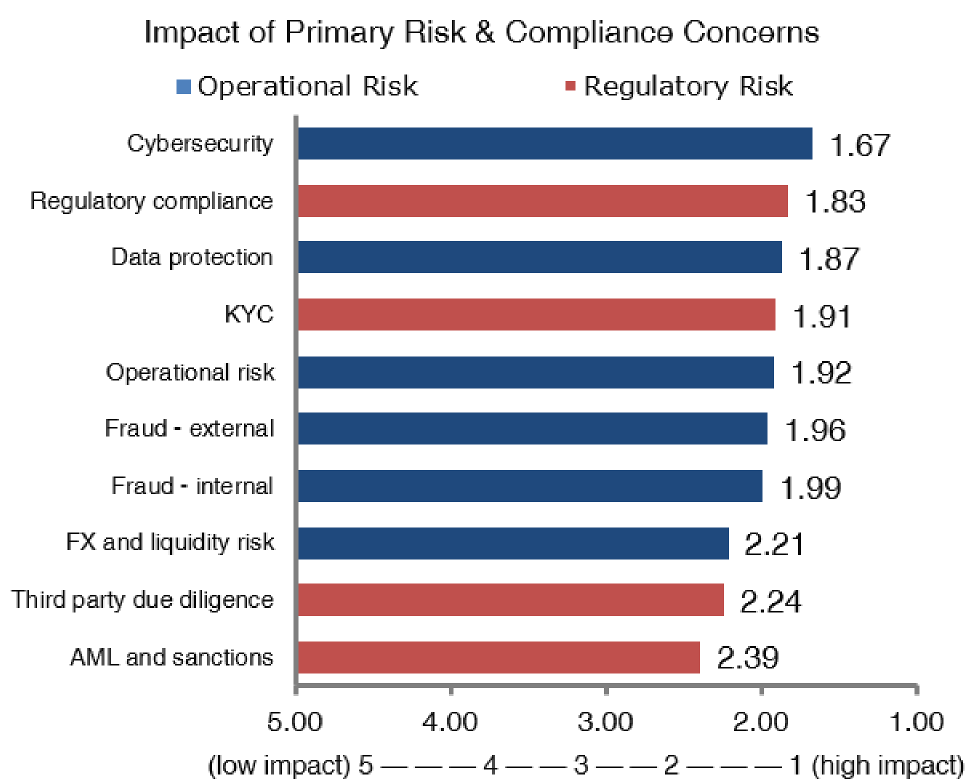
RESEARCH PARTNER

I. The big risk and compliance concerns for Asia Pacific corporates

- Cybersecurity is viewed as the risk and compliance concern impacting firms most adversely
- Significant regional differences present
- Regulatory compliance and KYC are following closely

Key concern impacting businesses: cybersecurity

Cybersecurity is the main risk and compliance concern across the Asia Pacific market however again, regional disparities are evident. Concerns around data protection has the most adverse impact for Hong Kong corporates while in Indonesia regulatory compliance is the area keeping corporates awake at night. Australia and Taiwan are both focused on cybersecurity.



**Whole of region*

The emphasis on cybercrime does not come as a surprise, with cyber research house Cybersecurity Ventures estimating global annual cybercrime costs will grow from USD$3 trillion in 2015 to USD$6 trillion by 2021. Spending on cybercrime prevention and services is similarly forecast to exceed USD$1 trillion over the next 5 years, helped along by recent high profile global attacks.

Although cybersecurity is seen as the main risk and compliance concern, regulatory compliance is a close second. With a complex legal system and fragmented bureaucracy, businesses in Indonesia are particularly concerned about the impact of regulatory compliance.

RESEARCH PARTNER

RESEARCH PARTNER

II. Cyber threats coming – are you ready!

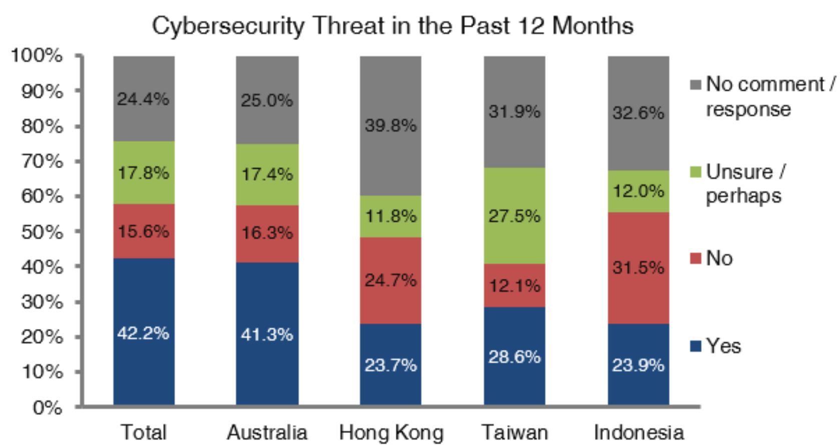
- Corporate risk managers lack the visibility to effectively assess their cybersecurity vulnerability
- Malware (including spyware and ransomware) and phishing lead as cyber threats
- Monetary loss outpaces data loss and identity theft as impacts of breaches

"What we don't know, we don't know unfortunately. Our surveillance systems aren't really where they need to be."

CFO, US$12Bn, Taiwan Semiconductor Manufacturer

Nearly half of all Asia Pacific corporates have experienced a cybersecurity threat over the last 12 months

Across the Asia Pacific region, only 15 percent of corporates claim with certainty that they have not experienced a cybersecurity threat over the past 12 months. This figure fell to 12.1 percent for Taiwan corporates and rose as high as 31.5 percent in the Indonesian market. However, the absence of evidence is not evidence of absence. The ease with which malware can be scaled, proliferate through networked computing and operate undetected suggests that corporates are overestimating their resilience to cyber threats. Also of concern, over 40 percent of corporates in the Asia Pacific region indicate either uncertainty around whether they had been the victim of a cyber-attack or were unwilling to comment, emphasising a low level of cyber awareness at the management level.

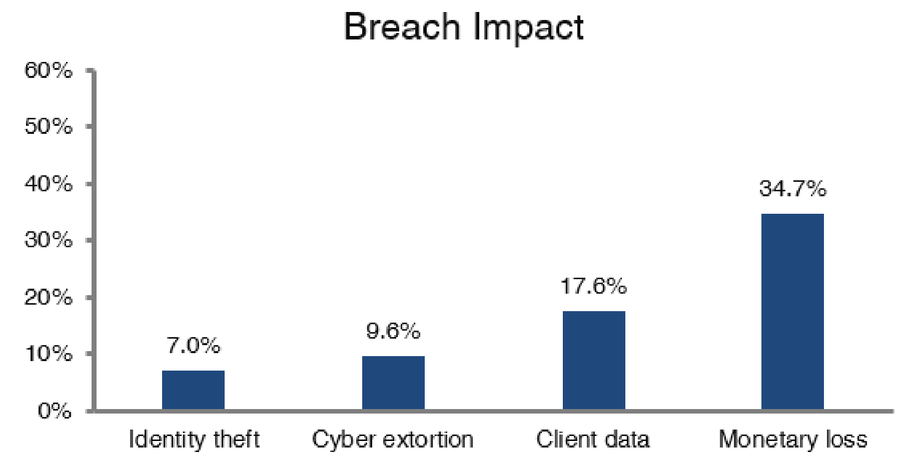


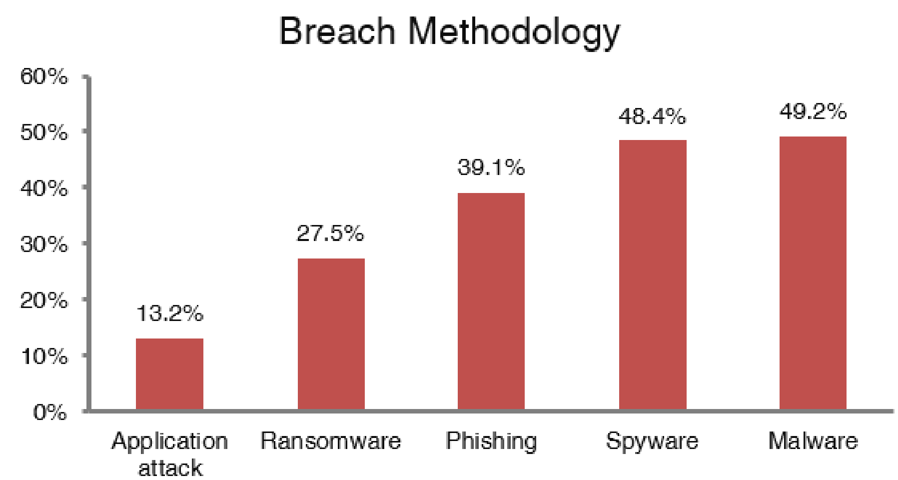
**Percentage of total Asia Pacific corporates and by indicated country, reporting on the incidence of cybersecurity threats experienced in the past 12 months.*

Monetary loss is the leading consequence of cyber breaches

Of the corporates who reported a cybersecurity breach over the past 12 months, malware, followed closely by spyware are the most common methods experienced market wide. Phishing, a technique attempting to gain access to sensitive information by impersonating communication from a trusted source, is more prevalent in more developed markets. Around 40 percent of corporates in Australia reported experiencing phishing attacks, falling to under 20 percent for Indonesian corporates.

Monetary loss is the key impact of breaches to corporates across the Asia Pacific region, suffered by one third of businesses who fall victim to cybersecurity attacks. Compared to other markets, Hong Kong corporates report a higher level of identity theft while Taiwan and Indonesian corporates experience more loss of client data.





**Percentage total does not sum to 100 percent due to multiple responses being allowed.*

The growing prevalence of cloud adoption, ever-expanding corporate databases, multiple touchpoints with external applications and the explosion of interconnected devices will only amplify data vulnerability and the perceived gains by those carrying out cyber-attacks. According to the Chief Information Officer (CIO) of the US Federal Communication Commission (FCC), it is estimated that the volume of digital content will rise 24 fold to 96 zettabytes by 2022 from 2017 levels. If corporate exposure and vulnerability to breaches is not addressed in the near term, as the volume of data available to would-be attackers grows, so too will the level and frequency of loss.

RESEARCH PARTNER

Risk and Compliance Index

Executive Summary

Key Takeaways

The big risk and compliance concerns for Asia Pacific corporates

Cyber threats coming – are you ready!

Your regulatory compliance behaviour

Risk management benchmarks

Research outline and Interviewee profile

III. Your regulatory compliance behaviour

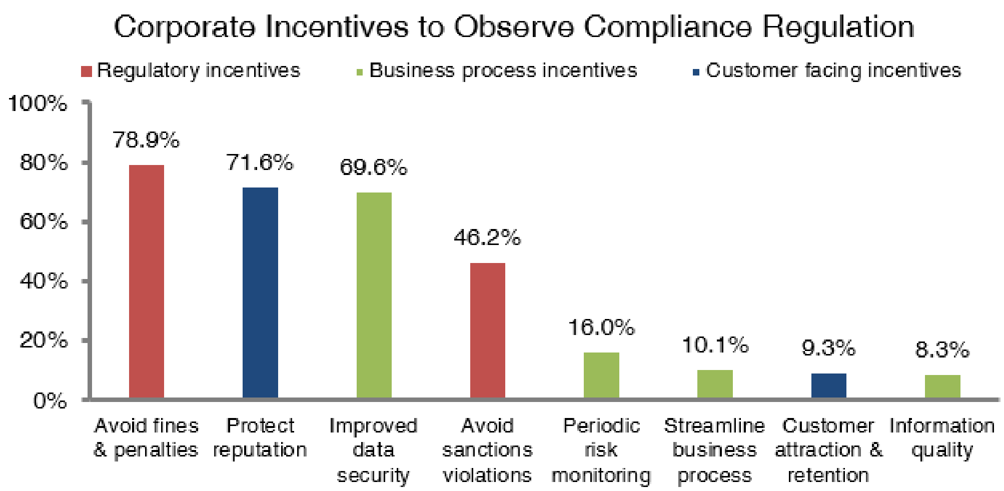
- Fine and penalty avoidance remains the primary driver of regulatory compliance
- Around half of corporates view risk and compliance as the primary responsibility of banks
- South East Asian corporates markedly accentuate the risks of internal over external fraud

"Although we understand and recognise these issues, our board is not yet ready to invest, so we have all these risk and compliance functions hidden inside the CFOs office – just not enough exposure to their importance yet internally."

CTO, US$2Bn Indonesian food group

Avoiding fines and penalties the key incentive to observing compliance regulation

Fine and penalty avoidance is consistently recognised as the primary motivating factor for adhering to regulations governing compliance, cited by nearly four fifths of Asia Pacific corporates. This is followed by management of reputational risk (71.6 percent) and improved data and informational security (69.6 percent). While financial risks are the leading motivation for corporates, more than two thirds of businesses also cite risks around both reputation and security, emphasising that most corporates are kept awake by more than one concern.



Significant variance is present between key markets in the Asia Pacific region, highlighting the differing cultural norms and difficulty in prescribing to a 'one size fits all' approach. Reputational risk is nominated most prominently by Australian and Hong Kong corporates (70.7 and 79.6 percent respectively), while Indonesian firms rank it as a diminutive fourth in importance. Conversely the quality of information and data is a much bigger incentive to Indonesian corporates (15.2 percent) than it is to businesses in other parts of the region.

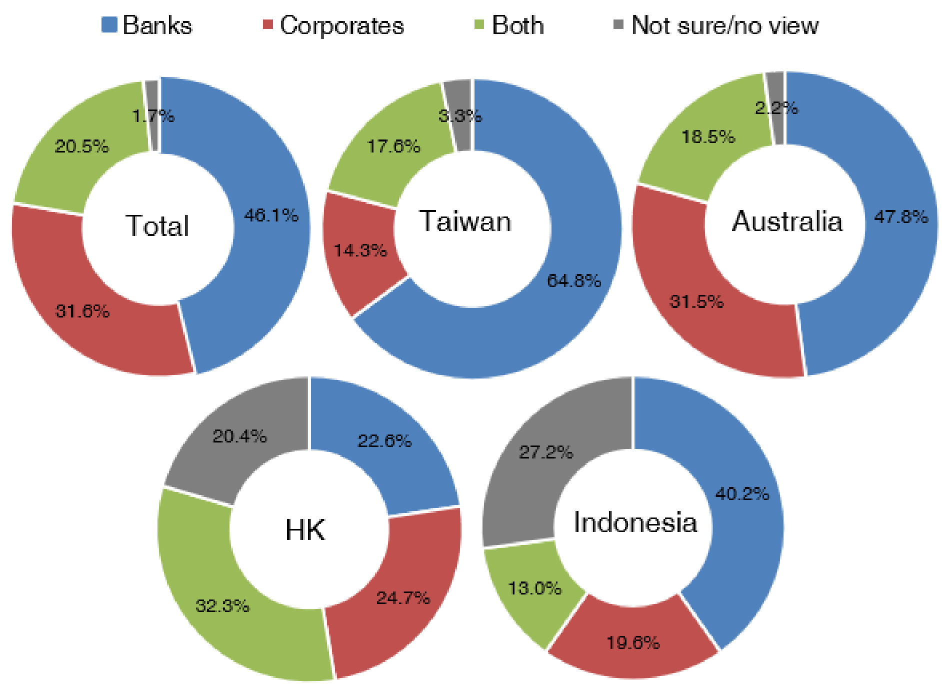
Banks lumped with responsibility of corporate compliance

Despite significant perceived risks to the corporates themselves, nearly half (46.1 percent) of firms across Asia Pacific think compliance is primarily the responsibility of banks. Again, intra -regional comparisons reveal stark differences in attitudes on this measure. The majority (64.8 percent) of Taiwan based corporates place compliance responsibility squarely on banks whereas in Hong Kong there is a more even split between banks and the corporates themselves for who is in charge of compliance issues.

RESEARCH PARTNER

Of concern in Hong Kong however is the large number of corporates (20.4 percent) who aren't sure where responsibility is designated, this uncertainty is also evident among Indonesian business (27.2 percent). If there is no clear party holding responsibility, corporates take the risk of opening themselves up to greater infringements of the regulations simply because they didn't know who was responsible for monitoring their actions.

Primary Compliance Responsibility



RESEARCH PARTNER

IV. Risk management benchmarks - call for improvement

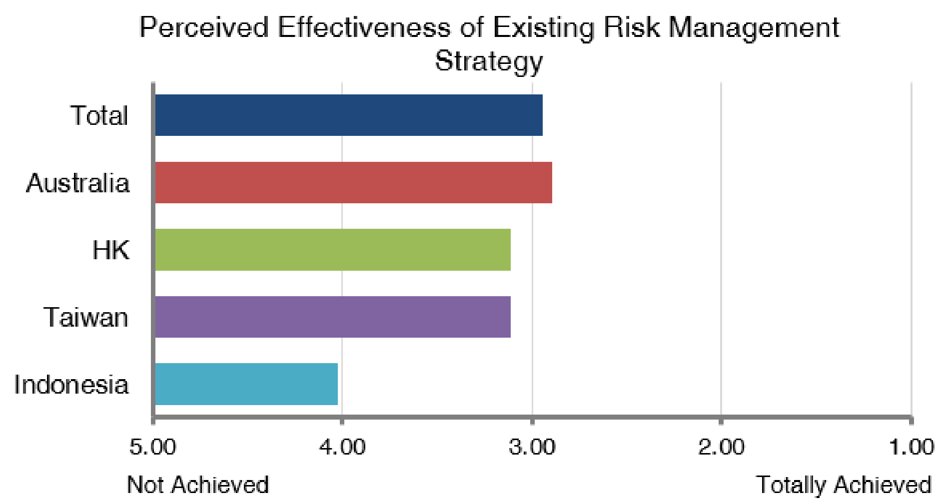
- High cyber breach incidence and impact reflects low risk management effectiveness
- Integrating risk and compliance into business processes remains the primary priority
- Low levels of risk preparedness carry a potentially significant reputational and financial cost

"We are very aware of the costs and risks in not having our compliance at best practice but getting proper funding to resource this is a problem."

Chief Risk Officer, US$4.5Bn Malaysian Conglomerate

Current risk management strategies seen as ineffective

Market-wide, corporates view the effectiveness of their existing risk management strategies as relatively mediocre. On a reverse scale of 1 (totally achieved) to 5 (not achieved), Asia Pacific corporates rate their strategies effectiveness as 2.94. Not surprisingly, corporates in developing markets such as Indonesia (4.02) report some of the lowest levels of effectiveness, whereas thos in Australia come in as just above the market average with a rating of 2.89.

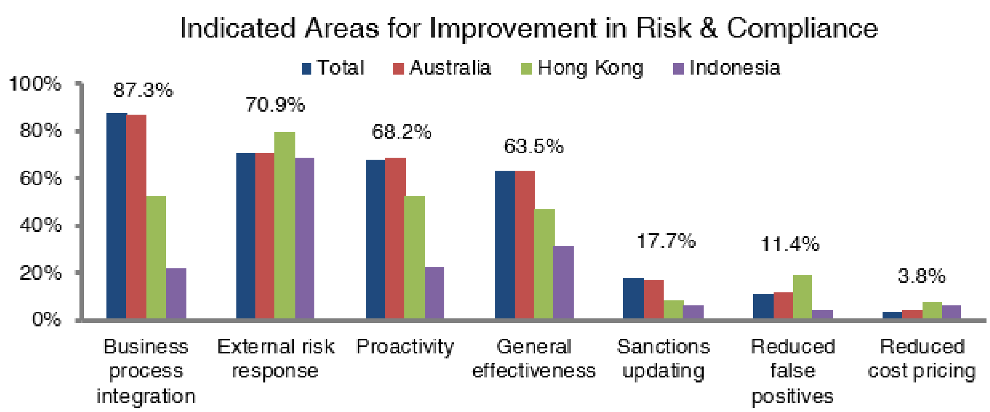


**Self-assessed rating of existing corporate risk management effectiveness as reported by the total sample of Asia Pacific corporates and by indicated country.*

Integrating 'risk and compliance management' more fully into

For corporates, integrating risk and compliance processes into the business more completely is the key area identified for improvement in their already existing strategy. This was followed by improving external risk assessment, highlighted by 70.9 percent of businesses. Despite Australian corporates viewing their existing risk management strategies the most favourably across the region, they identified significantly more areas for improvement than their regional counterparts. Improving the effectiveness of current measures, getting more proactive, integrating risk and compliance into the business more and improving external risk assessment are each nominated by over 60 percent of Australian corporates. All these key factors play into one another, corporates need to be more proactive to integrate risk management and compliance into their business further, which entails having both vendors and tools at their disposal to monitor risks and improve risk assessment.

RESEARCH PARTNER



**Percentage of total Asia Pacific corporates and by indicated country, reporting indicating intention to improve risk and compliance management processes listed.*

**Percentage total does not sum to 100 percent due to multiple responses being allowed.*

Gaps in risk and compliance governance were also identified in the management of newly identified risks. Over half of corporates indicate no existing standardised internal procedure with no plans to implement one, rising to an astonishing 80 to 90 percent in Taiwan and Indonesia. Whereas developing markets report lower incidences of cybersecurity breaches, they are more likely to suffer monetary or informational loss when they occur. While CFOs and Treasurers in lower risk countries may fall into complacency, there is a very real risk for potentially high reputational and financial burden should they fall victim to a sophisticated cyber breach.

How to resource the fight – internal or external

- Specialist advisers and vendors overwhelmingly preferred over banks for external risk advice
- Corporates prioritise reputation and effectiveness over cost factors in external providers
- Chief Risk Officers more prevalent across Australia

"We have gotten recognition at Board level around the commercial threats that exist in non-compliance with regulatory requirements. Cybersecurity has dominated things internally but general compliance is now top of the agenda."

Legal advisors are the source of most external risk management advice

Corporates in Asia Pacific, especially those in Australia and Taiwan, are increasingly turning to external providers for risk management and are favouring specialist providers over banks. Where corporates do turn to external providers, 25 to 35 percent indicate preferences for legal advisors, technology vendors and specialist consultants. This compares to below 8 percent for either compliance vendors or banks. Eschewing external providers, over a quarter of Hong Kong, and over half of Indonesian corporates rely wholly on internal risk management providers.

When selecting external providers to manage identified risks, reputation and expertise are corporates' top priorities. In comparison, cost and past experience with the provider are the least important factors to Asia Pacific corporates.

RESEARCH PARTNER

Risk and Compliance Index

Executive Summary

Key Takeaways

The big risk and compliance concerns for Asia Pacific corporates

Cyber threats coming – are you ready!

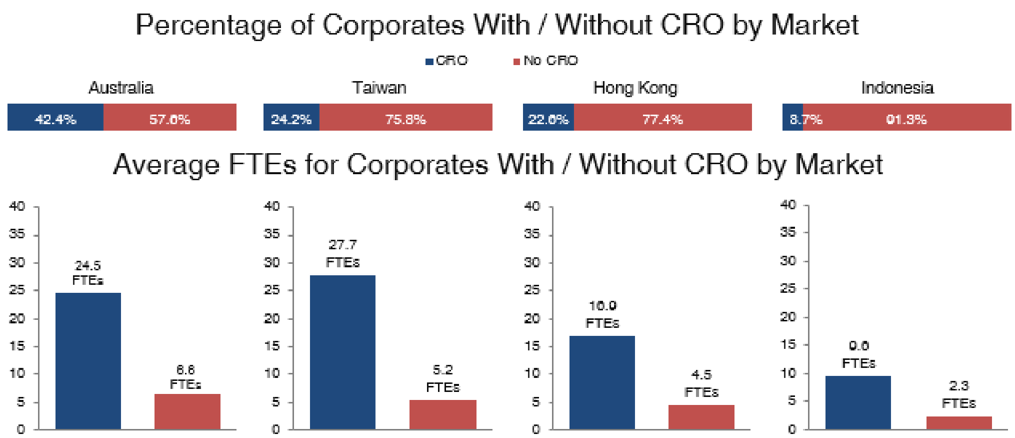
Your regulatory compliance behaviour

Risk management benchmarks

Research outline and Interviewee profile

Chief Risk Officers not yet the norm across Asia markets

Across Asia Pacific dedicated Chief Risk Officers (CRO) are currently only prevalent across the Australian market with just under half of corporates (42.4 percent) reporting they have one in place. The relatively mature market of Hong Kong is aligned with their Asia peers in that risk and compliance is not yet seen as having C-level importance but is more often than not relegated to the IT department. Not surprisingly, corporates with a CRO have a significantly higher risk and compliance FTE headcount than those without. Corporates with a CRO employed on average 23 FTE underneath the C-level executive, those without averaged 6 FTE. Regional differences are again apparent with Indonesian corporates having, on average, a lower headcount regardless of whether or not there was a CRO.



** Percentage of Asia Pacific reporting corporates by country with and without a designated Chief Risk Officer (CRO) (top), and associated annual risk and compliance headcount (bottom).*

Calls to corporate action

Managing risk and compliance will undoubtedly remain an ongoing challenge for CFOs, Treasurers and designated risk officers going forward. Every enterprise must assess the appropriate measures to be undertaken in response to mounting cyber threats and cybersecurity risk. The appropriate manner and scope of their response must reflect regulatory, cultural and market specific considerations. The widespread nature of cyber infractions and the ever-present risk of fraud represents a unifying incentive for stronger corporate governance practices.

Corporates across the region need to take greater responsibility and control of their regulatory compliance and minimise their reliance on their banking partners. The threats to corporates who do not are exponential both in terms of commercial fines and reputational risks. Taking greater control also extends to current risk management strategies, if these are ineffective steps need to be taken to improve existing processes.

The growth in data volume reflects the increase in cybersecurity threats and breaches. Corporates should expect to experience an ever-increasing number of incidents by way of an evolving range of threats. Corporates not only need to be able to quickly identify threats but be able to effectively remedy and/or contain any successful attacks should they occur.

"Our focus really is on customer and reputational risk in the markets should we have a major breach or event. We're trying to be as transparent as we can in communicating where we are on these issues with all our stakeholders."

CFO, US$5Bn Australian Logistics Group

RESEARCH PARTNER

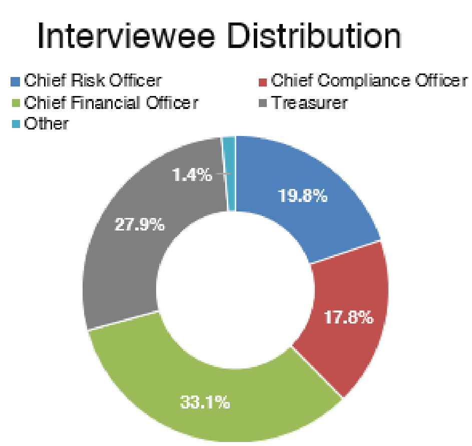
Research outline and Interviewee profile

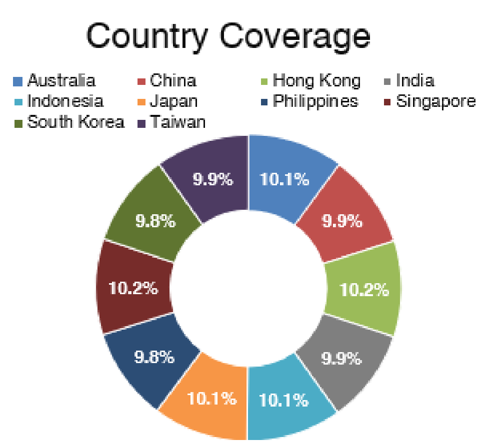
SWIFT commissioned industry research firm East & Partners to generate unique and valuable insights into corporate governance, risk and compliance management across Asia Pacific. This research into corporates explores existing risk management procedures and drivers, perceived readiness and cybersecurity vulnerability, and utilisation of internal and external risk management processes. Insights are designed to facilitate greater understanding of risk vulnerabilities, unmet corporate needs and areas of priority for SWIFT's financial and corporate customers.

Reporting is based on direct interviews with 915 corporates surveyed evenly across the 10 major economies in the Asia Pacific region, comprising Australia, China, Hong Kong, India, Indonesia, Japan, the Philippines, Singapore, South Korea and Taiwan. The target population was segmented against the Top 100 revenue ranked corporates in each country. Industry allocation was segmented against country specific concentrations, with prominent representation by Manufacturing, Wholesale Trade, Finance & Insurance, Retail Trade and Construction. Research was executed over a three-week period ending 17 May 2017.

Industry Sector Distribution			
Manufacturing	25.8%	Personal & Business Services	2.1%
Wholesale Trade	12.3%	Agriculture, Forestry & Fishing	2.0%
Finance & Insurance	10.6%	Govt. Administration & Defence	2.0%
Retail Trade	10.1%	Mining	1.9%
Construction	9.4%	Electricity, Gas & Water Supply	1.3%
Transport & Storage	9.3%	Accommodation, Cafes & Restaurants	0.7%
Property & Business Services	9.1%	Education	0.3%
Communications Services	3.0%	Health & Community Services	0.3%

Industry sector percentage segmentation for the full research sample. Intra-regional country distribution was segmented against the market's Top 100 revenue ranked corporates (N:915).





Interviewee role segmentation for the full research sample (left). Intra-regional interviewee variation varied according to industry segmentation. Country coverage distribution (right).

RESEARCH PARTNER

East & Partners Asia (Haymarket Pte Ltd), a leading specialist market research and consulting firm in the business, corporate and investment banking markets of Asia Pacific, works across 10 countries in the region delivering both multi-client and proprietary market analysis services to two sectors - Financial Services and Travel Hospitality.

The delivery of accurate quantitative analysis on the region's exploding demand for sophisticated transaction, debt, treasury, investment and advisory banking services and products and corporate T&E solutions is uniquely addressed by East's "bottom up" research methodologies, based on many thousands of customer interviews annually in China, Hong Kong, India, Indonesia, Malaysia, Philippines, Singapore, South Korea, Taiwan and Thailand.

East clients look for accurate assessments of these two Asian markets, addressing requirements for primary, customer-centric, high quality analysis amongst service and product providers. East's coverage of both sectors is "top to bottom" from Micro/SME business, through middle market Corporates to the large Institutional, "Top 1,000" segment.

East's multi-client demand research and consulting work has enabled the firm to work with virtually every major Bank within the region, international clients based in North America and Europe, international and local hotel chains, airlines and tourism boards. The joint venture firm combines the assets of East & Partners in research and analysis with those of Haymarket Media in the "Corporate Treasurer", "Finance Asia", "Asian Investor" and "CEI Asia" publishing and events platforms across Asia.

East Haymarket Pte Ltd

21 Media Circle, #05-05 Infinite Studios, Singapore 138 562

ABOUT SWIFT FOR CORPORATES

SWIFT for Corporates offers a wide and growing range of products and services for multibanked corporates to connect with banks and financial institutions through a single, secure and reliable channel. SWIFT provides corporate treasurers and finance managers global visibility on cash and trade, lower cost of financial transactions and improved security and reliability for their financial network.

For more information, visit http://corporates.swift.com/

ABOUT SWIFT

SWIFT is a global member-owned cooperative and the world's leading provider of secure financial messaging services.

We provide our community with a platform for messaging and standards for communicating, and we offer products and services to facilitate access and integration, identification, analysis and financial crime compliance.

Our messaging platform, products and services connect more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories, enabling them to communicate securely and exchange standardised financial messages in a reliable way.

As their trusted provider, we facilitate global and local financial flows, support trade and commerce all around the world; we relentlessly pursue operational excellence and continually seek ways to lower costs, reduce risks and eliminate operational inefficiencies.

Headquartered in Belgium, SWIFT's international governance and oversight reinforces the neutral, global character of its cooperative structure. SWIFT's global office network ensures an active presence in all the major financial centres.