中國香港網絡安全協會
HONG KONG CHINA NETWORK SECURITY ASSOCIATION

SIA

CYBERSECURITY BEYOND THE TOOLS:

Investments, Vendors Selection, And Strategic Decision-Making In Hong Kong

A study on how cybersecurity leaders in Hong Kong select, adopt, and derive value from cybersecurity solutions, and what the data, the practitioners, and the vendors tell us about the road ahead.

Foreword of the Chairman

David Ip
Founding Chairman
Hong Kong China Network Security Association

Mr. David Ip is the Founding Chairman of the Hong Kong China Network Security Association. He is devoted to promoting the formulation and implementation of regulations and industry standards for cybersecurity and creating a favorable environment for the development of the industry.

David held **senior positions in a number of leading global cyber security companies** where he was responsible for strategic planning and market growth for the global market.

David holds a degree in Computer Science from University College London, UK. He is a frequent public speaker at global conferences, sharing his knowledge and experience in cybersecurity and China digital marketing.

As **Hong Kong's first cybersecurity and data privacy community**, our mission has been clear from day one. To overcome our shared digital challenges, we have continuously bridged gaps across all sectors, leveraging our members' diverse backgrounds to share vital knowledge, tips, and real-world experiences.

Cybersecurity in Hong Kong has reached an increasingly critical yet complex juncture. We are all grappling with escalating threats, major regulatory overhauls, and a persistent, industry-wide talent shortage. Despite these immense pressures, most organizations continue to face flat budgets. This creates an intense operational tension between expanding security responsibilities and severely limited financial flexibility.

To address this friction, our Research Committee - led by Mr. Stefano Fois, Director of the Research Committee - spearheaded this milestone study. It marks a historic moment for our community, as this is the very first time any organization in Hong Kong has ever conducted research of this nature. Moving beyond theoretical frameworks, this study focuses explicitly on **how cybersecurity leaders make high-stakes, real-world decisions under budget constraints, intense regulatory scrutiny, and a fast-moving threat landscape**. It examines the practical, pressured choices leaders must make in an environment where the pace of change far exceeds any single organization's standalone capacity to respond.

The findings of this ground-breaking survey are unprecedented. As AI continues to rapidly amplify the speed and effectiveness of cyber attacks, the insights uncovered here demand serious, immediate attention from organizations of all sizes. In this new era, "assume breach" is no longer just a technical concept - it is a **critical, strategic reality and a frequent discussion I now have with stakeholders across every tier of leadership.**

I invite you to use this first-of-its-kind study as a practical roadmap to navigate these turbulent times, strengthen your organizational resilience, and protect our shared digital future.

Preface

Wilson Tang
Vice Chairman
Hong Kong China Network Security Association

Wilson is an industry leader with nearly **20 years of experience in cybersecurity.** As the CISO of one of the major telco operators in Hong Kong, Wilson leads the Information Security team on threat hunting, minimize cyber risk and building a security aware culture. Wilson believes that proactiveness and bringing value to talents are the key factors to success. Prior to his current role, Wilson served an international consulting firm for 5 years and a local system integrator for 15 years.

Wilson sees the advancement of network security in Chinese vendors while at the same time see Hong Kong lack a platform for security experts from different industries to share their experience, and that's the reason Wilson joined the Association hoping to learn more from different experts and share his valuable experience.

At the early stage of HKCNSA, I kept telling our Founding Chairman, David, that we needed to **produce tangible deliverables**, as this is what would create a meaningful impact on the industry.

In July 2025, with the support and commitment of Sia, we issued our first **Cybersecurity Talent Landscape in Hong Kong report**, a survey aimed at understanding the current challenges in the cybersecurity workforce landscape and how they could be addressed.

We then came up with the idea of conducting research on the selection of cybersecurity tools in Hong Kong, at a particularly important time marked by the **advancement of Chinese technology** and evolving geopolitical dynamics.

This was especially challenging for HKCNSA as a non-profit organization. We do not have a dedicated research budget, nor do we want to be sponsored to produce predetermined reports. Too often, we see reports that describe ideal scenarios and success stories, but remain distant from the true voice of the field. **The Hong Kong cybersecurity industry deserves a report that reflects the real situation** and helps us face challenges from different perspectives.

When we started planning this report, we were concerned about whether we could gather enough industry leaders willing to openly share their experiences, challenges, and solutions. We were too used to celebrating our achievements while hiding our weaknesses. It turned out that I had worried too much. Through our efforts to create a comfortable and trusted environment, we were able to encourage contributors from different fields to freely share their experiences and ideas for this report.

Together, we win. No one can survive alone.

Table of Contents

Introduction

Cybersecurity in Hong Kong has never been more consequential, or more complex. The city faces an **accelerating threat environment**, a **regulatory landscape** undergoing its most significant transformation in a decade, and a **structural talent crisis** that shows no sign of easing. And yet, most organizations continue to operate under budget constraints that have remained essentially flat. The result is a sector caught in a profound tension: growing obligations, shrinking room for manoeuvre, and a pace of change that outstrips the capacity of any single organization to keep up.

This study was born from a straightforward but important question: **how do cybersecurity leaders in Hong Kong actually make decisions?** Not in theory, not according to best-practice frameworks, but in practice, under budget pressure, regulatory scrutiny, talent constraints, and the relentless pace of a threat landscape that does not pause for planning cycles.

To answer that question, **the Hong Kong China Network Security Association (HKCNSA) and Sia joined forces** to conduct one of the most comprehensive studies of cybersecurity investment and vendor selection ever undertaken in the Hong Kong market. The research draws on **four distinct but complementary sources of insight:** (1) a **survey** of approximately one hundred cybersecurity professionals active across Hong Kong's key industries; (2) five in-depth **case studies** with organizations that have navigated significant cybersecurity tool selection and adoption programmes; (3) six candid **interviews** with cybersecurity solution vendors, including both Mainland Chinese and Hong Kong-based providers, on how they perceive and engage with the local market; (4) and structured interviews with **three senior cybersecurity leaders**, whose accumulated wisdom forms the backbone of the study's final chapter.

What emerged from this research was richer and more complex than we anticipated. The data does not simply describe a market investing in cybersecurity. It reveals a market under tension, between ambition and resource, between compliance and strategy, between the tools organizations are buying and the foundations they have yet to build. **Six structural tensions** crystallize from the survey findings, each one interconnected, each one shaping the others in ways that define the current state of the sector.

At the same time, the practitioner voices in this study offer something that data alone can not: the texture of lived experience. The

case studies document real procurement decisions, real deployment challenges, and real lessons learned, including lessons about the growing role of Mainland Chinese cybersecurity solutions in the Hong Kong market, and the nuanced, category-specific judgements that effective vendor selection requires. The vendor perspectives add a further dimension, revealing how the supply side of the market perceives its own challenges, its own opportunities, and the structural dynamics that will shape the next three to five years.

This study does not resolve the tensions it identifies. It maps them, because understanding the terrain is the first step to navigating it.

What it offers instead is **rigor, honesty, and the kind of grounded, practitioner-validated insight that can help cybersecurity leaders make better decisions**, about where to invest, how to select vendors, how to build the governance infrastructure that makes security investments work, and how to navigate a market that is changing faster than any single organization can track alone.

The findings are presented across **five parts**, each building on the last. Readers are encouraged to engage with the study as a whole, because it is in the connections between the data, the cases, the vendor perspectives, and the practitioner wisdom that the most important insights emerge.

The Methodology of the Study

Following the publication of **"The Cybersecurity Talent Landscape in Hong Kong"** in June 2025, the Hong Kong China Network and Security Association (HKCNSA) and Sia partnered to undertake a new study, one that responded directly to a need expressed by the practitioner community. Through ongoing conversations with cybersecurity professionals across Hong Kong, a clear demand had emerged: **more rigorous, evidence-based research into how organizations select, adopt, and derive value from cybersecurity solutions**. This study is the response to that demand. It draws on four distinct but complementary strands of inquiry, each designed to capture a different dimension of the cybersecurity investment landscape.

1. The Survey

The foundation of this research is a dedicated survey, sent to approximately one hundred cybersecurity professionals active in Hong Kong. The survey was designed to examine how organizations allocate spending across key security domains; how they navigate build-versus-buy decisions; and how or whether they measure the return on their security investments. It also explored vendor selection practices in depth, including the criteria applied, the due diligence processes followed, and the most common challenges encountered. A forward-looking component mapped emerging priorities and anticipated investment shifts over the next 24 to 36 months.

2. Practitioners' Deep Dive Case Studies

To complement the findings with lived experience, **five senior cybersecurity leaders working in different sectors in Hong Kong** were invited to participate in in-depth qualitative interviews. These practitioners shared detailed accounts of their direct experiences in selecting and adopting cybersecurity tools, including the challeng-es they encountered, the lessons they learned, and the best practices they have developed over time. Their insights provide the texture and specificity that survey data alone cannot capture, and form the basis of the case study material presented through-out this report.

3. The Vendor Perspectives

The study also sought to **understand the supply side of the Hong Kong cybersecurity market**. **Six cybersecurity solution vendors were interviewed**, including both locally based vendors and vendors originating from Mainland China, to explore how Chinese-developed solutions are being positioned and received in the Hong Kong market, how vendor-client relationships are evolving in this context, and what vendors themselves anticipate for the future of the market. This perspective adds an important dimension to the analysis, situating buyer behavior within the broader commercial and geopolitical landscape in which it takes place.

4. Expert Points of View and Forward-Looking Recommendations

In the final stage of the research, **a group of senior cybersecurity leaders** were invited to review the study's findings and offer their **reflections, recommendations, and points of view**. Their contributions, grounded in deep professional experience and informed by the research findings, are presented as **practical guidance** for cybersecurity professionals and the broader community, with a particular focus on the decisions and priorities that will matter most in the years ahead.

Confidentiality and Anonymization

We sincerely appreciate the contributions of all professionals who dedicated their time and expertise to this study. In equal measure, we are fully committed to respecting the confidentiality of the information they shared. The data collected, in particular from survey results and practitioner interviews, has been anonymized where requested. Under no circumstances will the Research Team breach the confidentiality agreed upon with participants.

The Structure of the Study

The study is composed of five main parts, each addressing a distinct dimension of the cybersecurity investment and vendor selection landscape in Hong Kong. Together, they form a progressive and integrated analysis, moving from context and data, through lived experience and market perspective, to practical wisdom and forward-looking guidance.

Part 1. Context: The Current State of Cybersecurity in Hong Kong

The study opens by establishing the **environment in which cybersecurity decisions in Hong Kong are made**. This section briefly examines the threat landscape, including the accelerating volume and sophistication of cyberattacks targeting the city, alongside the regulatory environment, which has been fundamentally reshaped by the landmark **Protection of Critical Infrastructures (Computer Systems) Ordinance (PCICSO)**, in force since January 2026. It also addresses the structural talent shortage that constrains organizations across all sectors, and the technology transition driven by cloud adoption and artificial intelligence. This context is not background, it is the essential lens through which all subsequent findings must be read.

Part 2. Survey Findings: The Six Forces Shaping the Cybersecurity Investment Landscape

Drawing on the survey of approximately one hundred cybersecurity professionals, this section identifies **six structural tensions** that define the current state of cybersecurity investment in Hong Kong: (1) the gap between budget stability and strategic ambition; (2) the dominance of compliance as an investment driver; (3) the widespread inability to measure return on security investment; (4) the paradox of in-house GRC management combined with chronic

underinvestment in it; (5) the talent crisis that is acknowledged but systematically underfunded; (6) and the gap between AI ambition and operational readiness. Each tension is examined in depth, with data, analysis, and implications for cybersecurity leaders and vendors alike.

Part 3. Voices from the Ground: Experiences from Cybersecurity professionals

Five Hong Kong-based organizations share their firsthand experiences of selecting and deploying cybersecurity solutions, with a particular focus on tools originating from Mainland China. The cases span financial services, multinational corporations, and technology-driven enterprises, and cover decisions ranging from DNS security and endpoint protection to collaboration platforms, attack surface management, and large-scale SASE transformation. Cross-cutting themes, including the non-negotiability of structured procurement, the centrality of geopolitical risk, and the importance of vendor relationships, are distilled into practical lessons for cybersecurity leaders navigating similar decisions.

Part 4. Beyond the Sales Pitch: What the Vendor Accounts Really Tell Us

Six cybersecurity solution vendors, spanning Mainland Chinese and Hong Kong-based providers, share their perspectives on the Hong Kong market: its opportunities, its structural challenges, and the trends they expect to shape it over the coming years. Their accounts are candid and, taken together, remarkably convergent. This section examines what vendors reveal about the perception barriers facing Chinese solutions, the role of geopolitics in opening and closing commercial doors, the importance of deployment support and partner capability, and the trajectory of the Chinese cybersecurity vendor market as a whole.

Part 5. Lessons from the Field: Practitioners' Wisdom and the Path Forward

The study closes with its most practically actionable chapter: a series of lessons drawn from in-depth interviews with three senior cybersecurity leaders operating in Hong Kong and the broader APAC region. Their insights address board communication, AI adoption, GRC modernization, vendor selection, technology roadmap governance, and the structural challenge of organizational silos. The chapter includes a comprehensive **vendor selection checklist** derived directly from practitioner experience, and closes with **five imperatives** for the cybersecurity leader of 2026 and beyond.

Acknowledgements

We extend our sincere gratitude to **all those who contributed to this study**, particularly the cybersecurity professionals who generously completed surveys, answered our questions, and shared their valuable insights. This research would not have been possible without their participation.

We are especially grateful to the **senior leaders** who invested their time and expertise to provide detailed accounts of their experiences. Their contributions added practical value to this study and furnished concrete examples of effective, and ineffective, approaches to vendor engagement and management.

While confidentiality prevents us from acknowledging contributors by name, we wish to express our deep appreciation to all professionals who, despite demanding schedules, committed their time to this initiative.

Finally, we thank the **cybersecurity vendors** who openly shared their perspectives and market insights. Their transparency and willingness to engage with the research community foster the direct, honest collaboration and partnership relationships that we identify as essential for the industry's future.

Part 1. Context: The Current State of Cybersecurity in Hong Kong

Hong Kong occupies a singular position in the global cybersecurity landscape. As one of Asia's premier financial centers, **a gateway between mainland China and international markets**, and a hub for professional services, logistics, and technology, the city presents a threat surface that is simultaneously broad, deep, and strategically significant. Understanding the current state of cybersecurity in Hong Kong is not merely background, it is the essential context without which the research findings cannot be properly interpreted.

A Threat Environment of Exceptional Complexity

Hong Kong's cybersecurity threat environment is shaped by forces that are unique to its geopolitical and economic position. The city sits at the **intersection of multiple threat vectors**: sophisticated state-sponsored actors targeting financial infrastructureand sensitive data; organized criminal groups exploiting the city's role as a financial intermediary; and opportunistic attackers drawn by the concentration of high-value targets across banking, insurance, legal services, and professional advisory firms.

The scale of the threat is not theoretical, it is measurable and accelerating. According to the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), **12,536 cybersecurity incidents were recorded in Hong Kong in 2024**, with phishing accounting for over half of all cases, 7,811 incidents, representing a **108% increase from 2023** and the highest level in five years[1]. Phishing links alone surpassed 48,000 in 2024, a **150% year-on-year rise**,

[1] HKCERT, "Hong Kong Cyber Security Outlook 2025", January 2025

with the banking, finance, and e-payment sectors being the primary targets[2].

By 2025, the situation had deteriorated further: HKCERT recorded **15,877 cybersecurity incidents** a new record high, marking a **27% year-on-year increase[3]**. In the first half of 2025 alone, **financial losses through cybersecurity crimes in Hong Kong reached HK 3.04 billion** (approximately US 387 million), a nearly **15% year-on-year increase[4]**.

The financial sector, which dominates Hong Kong's economy, is a particularly attractive target. Banks, asset managers, insurance companies, and securities firms hold vast quantities of sensitive financial data, process enormous transaction volumes, and maintain connections to global financial infrastructure that, if compromised, could have cascading consequences far beyond Hong Kong's borders. The Hong Kong Police Force received **more than 440,000 pieces of intelligence on cyberthreats targeting the city in 2024**, and found that **5% of network assets owned by critical infrastructure operators were vulnerable to online attacks[5].**

The **2024 deepfake fraud incident**, in which a Hong Kong finance worker at engineering group Arup was deceived into transferring **HK 200 million** (approximately US 25.6 million) to fraudsters using AI-generated video of company executives during a multi-person video conference call, illustrated with painful clarity the sophistication of the threats now facing organizations in the city[6]. Every participant on the call, including the simulated CFO and multiple colleagues, was a deepfake. The fraud was not discovered until the employee checked with the company's head office days later. Hong Kong police noted that deepfake-related fraud activity is on the rise, with at least 20 cases in the preceding year in which deepfake video was used to deceive facial recognition systems[7].

Ransomware attacks have also become an increasingly serious concern. Hong Kong organizations across multiple sectors, including healthcare, logistics, and professional services, have experienced significant ransomware incidents in recent years, with attackers demonstrating both technical sophistication and a clear understanding of which organizations are most likely to pay to recover their data and restore operations. The growing **professionalization of ransomware-as-a-service (RaaS)** operations has lowered the barrier to entry for attackers while raising the stakes for defenders. The

[2] FutureCISO, “Hong Kong's 5 cyber security risks for 2025”, January 2025
[3] HKCERT, “Hong Kong Cyber Security Outlook 2026”, January 2026
[4] SCMP, “Cybersecurity crime losses in Hong Kong up 15% year on year in first half of 2025”, July 2025
[5] Hong Kong Police Force, “Cybersecurity Report 2024”, June 2024
[6] SCMP, “‘Everyone looked real’: multinational firm’s Hong Kong office loses HK$200 million after scammers stage deepfake video meeting”, February 2024
[7] Hong Kong Police Force, The Government of Hong Kong SAR, “LCQ9: Combating frauds involving deepfake”, June 2024

HKCERT's 2025 Cyber Security Outlook specifically highlighted a notable increase in attacks on critical infrastructure, including a ransomware attack on a Hong Kong hospital in 2024. By 2025, malware cases in Hong Kong had **more than doubled**, becoming the fastest-growing threat category tracked by government data.

Supply chain vulnerabilities represent a third dimension of the threat landscape that is particularly acute in Hong Kong. As a trading and logistics hub, Hong Kong organizations maintain extensive networks of suppliers, partners, and service providers, each of which represents a potential entry point for attackers. The **SolarWinds** and **MOVEit** incidents demonstrated globally how supply chain compromises can affect thousands of organizations simultaneously, and Hong Kong's deeply interconnected business ecosystem makes it especially exposed to this category of risk. HKCERT has identified supply chain security as one of the **primary cybersecurity risks for Hong Kong in both 2025 and 2026**, noting that security vulnerabilities in third-party software, applications, and open-source code represent a growing and systemic threat.

The cumulative picture is one of a threat environment that is not merely growing in volume but evolving in sophistication. Hong Kong's **suspected digital fraud rate stood at 6.2% in 2024, 15% above the global average**, marking the **fifth consecutive year** the city has exceeded global fraud risk levels[8]. According to TransUnion's 2024 State of Omnichannel Fraud report, **Hong Kong ranked third globally in average fraud losses**, with residents suffering average financial losses exceeding HK 260,000 (approximately US 33,500), nearly **2.5 times the global average**.

The Regulatory Landscape: Complex, Evolving, and Demanding

Hong Kong's regulatory environment for cybersecurity is among the most complex in the Asia-Pacific region, and it is becoming more so. Organizations operating in the city must navigate multiple overlapping regulatory frameworks, each with its own requirements, timelines, and enforcement mechanisms.

The Personal Data (Privacy) Ordinance (PDPO), administered by the Office of the Privacy Commissioner for Personal Data (PCPD), establishes the foundational framework for data protection in Hong Kong. Recent amendments have strengthened

[8] TransUnion, "2024 State of Omnichannel Fraud", May 2025

the ordinance's provisions around data breach notification and cross-border data transfers, increasing the compliance burden on organizations that handle personal data, which, in practice, means virtually every organization of any size.

The Hong Kong Monetary Authority (HKMA) has been particularly active in driving cybersecurity standards across the banking sector. Its Cybersecurity Fortification Initiative (CFI) 2.0, launched in 2021, established a comprehensive framework for assessing and improving the cyber resilience of authorized institutions. The CFI 2.0 framework includes a Cyber Resilience Assessment Framework (C-RAF), a Professional Development Programme (PDP), and an Intelligence-Led Cyber Attack Simulation (iCAST) programme, together representing one of the most sophisticated regulatory cybersecurity frameworks in the region.

The Securities and Futures Commission (SFC) has similarly strengthened its cybersecurity requirements for licensed corporations, with particular emphasis on operational resilience, incident reporting, and the security of client data. The SFC's circular on cybersecurity sets out detailed expectations for governance, risk management, and technical controls that licensed firms must meet.

The Protection of Critical Infrastructures (Computer Systems) Ordinance (PCICSO), Hong Kong's first dedicated cybersecurity law, represents the most significant regulatory development in the city's cybersecurity history. Passed by the Legislative Council on **19 March 2025** and coming into full force on **1 January 2026**, the Ordinance establishes a mandatory statutory framework for the protection of critical computer systems across **eight designated sectors: energy, information technology, banking and financial services, air transport, land transport, maritime transport, healthcare services, and telecommunications and broadcasting**. A new **Office of the Commissioner of Critical Infrastructure (Computer-system Security)** has been established to oversee and enforce the regime, with the Commissioner empowered to designate Critical Infrastructure Operators (CIOs) and Critical Computer Systems (CCSs), issue Codes of Practice, and investigate cybersecurity incidents.

The Ordinance imposes three categories of obligations on designated CIOs: **organizational obligations** (including maintaining a local office in Hong Kong and establishing a computer-system security management unit); **preventive obligations** (including regular security risk assessments, security management plans, independent audits at least once every two years, and penetration testing); and **incident reporting and response obligations** (including notification of serious cybersecurity incidents within 12 hours). Non-compliance carries penalties ranging from **HK 300,000 to HK 5 million**, with additional daily fines for continuing offences[9]. On 1 January 2026, the Commissioner simultaneously issued a **Code of Practice** that translates the Ordinance's high-level obligations into specific, actionable compliance requirements, marking a clear shift from principles to implementation.

[9] Hong Kong e-Legislation, January 2026

The significance of the PCICSO cannot be overstated. It represents **Hong Kong's first comprehensive, legally enforceable cybersecurity framework**, moving the city from a landscape of voluntary standards and sector-specific guidance to one of statutory obligations backed by enforcement powers. For organizations in the designated sectors, including the financial services firms that form the primary audience for this research, the Ordinance adds a further and substantial layer of compliance obligation to an already demanding regulatory environment. Critically, the Ordinance's supply chain provisions, which can extend its reach to computer systems located overseas but accessible from Hong Kong, and which require CIOs to flow down security obligations to their suppliers, have significantly implications for third-party risk management across the sector.

Beyond these Hong Kong-specific frameworks, organizations with operations or customers in mainland China must also navigate the requirements of **China's Cybersecurity Law (CSL), Data Security Law (DSL), and Personal Information Protection Law (PIPL)**, a trio of regulations that have significantly raised the compliance bar for cross-border data flows and critical information infrastructure protection. For many Hong Kong organizations, particularly those in financial services and professional services with Mainland operations, these requirements add a further layer of complexity to an already demanding regulatory environment.

The Talent Market: Scarcity in a Competitive Environment

Hong Kong's cybersecurity talent market is characterized by persistent scarcity and intense competition, a structural challenge that is well-documented and, by all available evidence, worsening.

The most comprehensive recent assessment of this challenge is the **report on the Cybersecurity Talent Landscape in Hong Kong**, published by Sia and HKCNSA in 2025. The report, which surveyed approximately one hundred cybersecurity professionals in Hong Kong and engaged professional recruiters with broad market knowledge, found that the talent shortage in Hong Kong is **systemic in nature**, driven by root causes that the city's unique context has not facilitated resolving . Critically, the report found that the talent shortage has driven up hiring costs, prompting organizations to seek more automation and outsourced services, particularly from locations outside Hong Kong where services can be provided remotely and labor is cheaper. This dynamic is directly visible in the survey data analyzed in this report, where outsourcing rates in operationally intensive domains such as security monitoring and threat detection are significantly higher than in governance-intensive domains.

The scale of the challenge is confirmed by multiple independent data sources. **Cisco's 2025 Cybersecurity Readiness Index** found that **only 1% of organizations in Hong Kong have achieved a mature level of cybersecurity readiness**, a figure that has not changed from 2024, highlighting a concerning stagnationin preparedness amidst growing threats[10]. Separately, **95% of respondents in Hong Kong cited a lack of skilled cybersecurity professionals as a challenge, with over half reporting more than ten open roles**, a figure that speaks to the depth and breadth of the talent gap across organizations of all sizes.

The global cybersecurity workforce gap, estimated by ISC² at approximately **4.7 million professionals worldwide[11]** is felt acutely in Hong Kong. The city's universities produce a limited number of cybersecurity graduates each year, and the pipeline of mid-career professionals with specialized skills in areas such as cloud security, threat intelligence, and AI security is even thinner. Organizations compete not just with each other but with global firms that can offer. remote work arrangements, higher compensation, and broader career development opportunities. A study by the Hong Kong General Chamber of Commerce found that **74% of Hong Kong's business leaders need more talent, with 60% identifying IT talent shortage as the biggest roadblock to adopting emerging technologies[12]**.

This talent scarcity is compounded by the rapid evolution of the threat landscape and the technology stack. Skills that were cutting-edge three years ago, in areas such as traditional network security or on-premises infrastructure protection, are now table stakes, while demand for expertise in cloud-native security, AI/ML security, and

[10] Cisco, “2025 Cisco Cybersecurity Readiness Index”, May 2025
[11] ISC2, “2024 Cybersecurity Workforce Study”, October 2024

operational technology (OT) security is growing faster than the talent pool can expand. The HKCNSA/Sia report specifically identifies this **skills evolution mismatch** as a key dimension of the talent challenge, organizations need professionals who can operate in an environment defined by AI-enhanced threats, complex multi-cloud architectures, and an expanding regulatory compliance burden, but the supply of such professionals is severely constrained[13]. The result is a market in which skilled professionals command premium compensation, organizations struggle to fill critical roles, and the gap between security ambitions and security capabilities continues to widen.

The talent challenge has a further dimension that is specific to Hong Kong: **the city's bilingual requirements**. English and Chinese (Cantonese and Mandarin), narrow the effective talent pool further, as cybersecurity professionals who can operate effectively across both linguistic and cultural contexts are particularly scarce. This bilingual requirement, combined with Hong Kong's high cost of living and the competitive pull of Singapore and other regional hubs, creates structural retention challenges that are difficult to address through compensation alone.

The Technology Transition: Cloud, AI, and the Architecture of the Future

Hong Kong's cybersecurity talent market is characterized by persistent scarcity and intense competition, a structural challenge that is well-documented and, by all available evidence, worsening.

Hong Kong organizations are in the midst of a significant technology transition that is reshaping the cybersecurity challenge. The **accelerating adoption of cloud infrastructure** (driven by cost efficiency, scalability, and the demands of hybrid work) has fundamentally changed the attack surface that organizations must defend. Traditional perimeter-based security models, designed for a world in which data and applications lived inside a defined network boundary, are increasingly inadequate for environments in which workloads span multiple cloud providers, data flows across geographic boundaries, and users access systems from anywhere.

The emergence of Artificial Intelligence as both a security tool and a threat vector adds another dimension of complexity. On the defensive side, AI-powered tools offer genuine promise for threat detection, behavioral analysis, and automated response, capabilities that are increasingly necessary given the volume and sophistication of modern attacks. On the offensive side, AI is enabling attackers to craft more convincing phishing campaigns, generate more sophisticated malware, and automate reconnaissance and exploitation at scale. HKCERT has specifically identified **AI-related attacks and AI content hijacking as top cybersecurity concerns for 2026[14]**, noting that the rise of generative AI has made phishing messages increasingly realistic and harder to detect, a direct contributor to the record phishing volumes recorded in both 2024 and 2025.

[13] HKCNSA & Sia Partners, “The Cybersecurity Talent Landscape in Hong Kong”, June 2025
[14] HKCERT “Hong Kong Cybersecurity Outlook 2026”, January 2026

The deepfake fraud incident previously described is a harbinger of a broader trend: **AI is lowering the cost and raising the effectiveness of social engineering attacks** in ways that traditional security awareness training is not equipped to address. The convergence of AI-enhanced offensive capability with Hong Kong's high-value financial sector targets creates a threat environment that is qualitatively different from what organizations faced even three years ago.

Hong Kong's Cybersecurity Market: Strengths and Forecasts

Despite these challenges, Hong Kong has genuine strengths in its cybersecurity ecosystem. The city has a **well-developed professional services sector** with deep expertise in risk management, compliance, and governance, capabilities that translate directly into cybersecurity. Its financial sector has been an early adopter of sophisticated security practices, driven by regulatory pressure and the high stakes of financial crime. And its position as a regional hub means that it has access to a wide range of international cybersecurity vendors, consultants, and managed service providers. The Hong Kong cybersecurity market is estimated at **USD 850 million in 2025**, forecast to grow at an **8.53% CAGR to USD 1.35 billion by 2031**[15], a trajectory that reflects both the scale of the challenge and the investment being mobilized to address it.

The Hong Kong government has also taken steps to strengthen the city's cybersecurity posture. The **Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT)**, operated by the Hong Kong Productivity Council, provides threat intelligence, incident response support, and security awareness resources to organizations

The Context for What Follows

It is against this backdrop, a complex and accelerating threat environment, a demanding and newly expanded regulatory landscape anchored by the landmark PCICSO, a constrained talent market with systemic structural challenges, and an accelerating technology transition driven by AI and cloud adoption, that the survey findings must be read.

The **six structural tensions** identified in this analysis are not abstract strategic puzzles. They are the lived reality of organizations navigating one of the most challenging cybersecurity environments in the world: a city where the threat is sophisticated and growing, where the regulatory burden isexpanding faster than compliance capacity, where the talent needed to respond is scarce and expensive, and where the technology investments required to keep pace are significant, complex, and difficult to justify without better measurement frameworks.

Understanding this context does not excuse the gaps the survey reveals. But it does explain them, and it is essential context for any honest assessment of what it will take to close them.

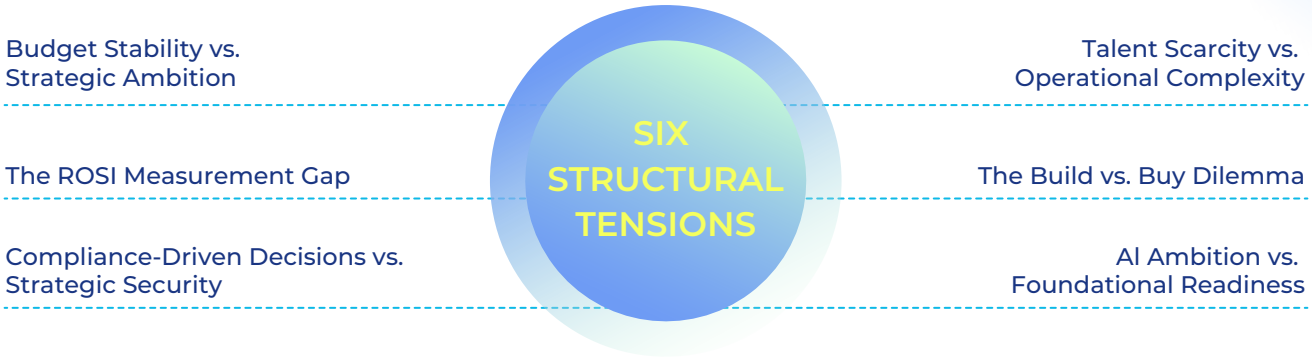
[15] Mordor Intelligence, “Hong Kong Cybersecurity Market Analysis”, January 2026
[16] Hong Kong Police Force, “Cybersecurity Report 2024”, June 2024

Part 2. Survey Findings: The Six Forces Shaping the Cybersecurity Investment Landscape

The survey sets out to explore how organizations approach cybersecurity solutions selection and adoption. What emerged, however, was a far richer and more complex picture, one that reveals deep structural tensions, strategic blind spots, and a sector navigating significant transformation under considerable pressure. Across 20 questions, respondents painted a portrait of an **industry that is simultaneously ambitious and constrained**, rigorous and reactive, **forward-looking and trapped by present-day limitations**.

Six key tensions crystallized from the data, and together they tell a story that goes well beyond tools and technology:

- **Budget Stability vs. Strategic Ambition** exposes the contradiction between flat resources and soaring investment plans.
- **Compliance-Driven Decisions vs. Strategic Security** reveals how regulatory pressure has become the dominant, and sometimes limiting, lens through which security choices are made.
- **The ROSI Measurement Gap** uncovers a sector that cannot yet demonstrate the financial value of what it spends, though organizations are increasingly turning to Business Impact Analysis (BIA) as their primary measurement tool.
- **The Build vs. Buy Dilemma** highlights a striking paradox: organizations outsource their most operationally intensive domains while keeping Governance, Risk & Compliance (GRC) stubbornly in-house despite underinvesting in it.
- **Talent Scarcity vs. Operational Complexity** shows how organizations are adding sophisticated tools and automation while systematically underfunding the human expertise required to operate them effectively.
- **AI Ambition vs. Foundational Readiness** captures the defining strategic risk of the moment: an industry racing toward AI-powered security futures without yet having resolved the foundational capabilities that will determine whether that future succeeds.



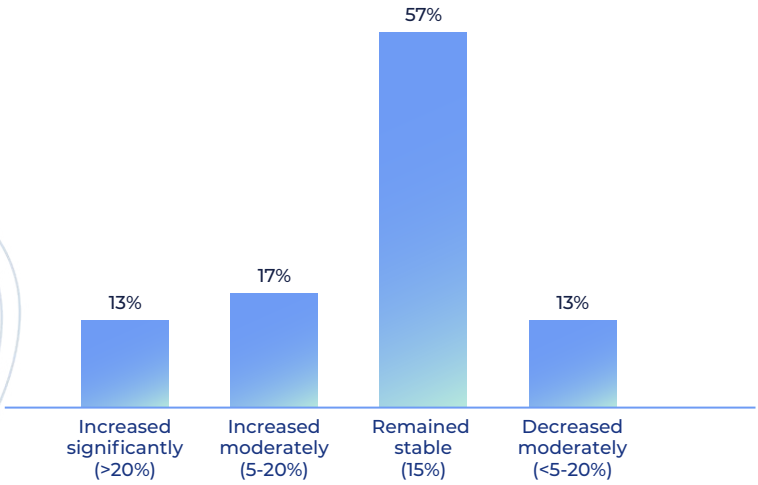
The Six Tensions

These six tensions matter not because they are isolated findings, but because **they are deeply interconnected**, each one reinforcing and amplifying the others in ways that shape the entire cybersecurity landscape. Understanding this intricate web is what makes this survey particularly valuable, and it is what this chapter sets out to illuminate.

The Organizational Context: Budget, Priorities and the Ambition Gap

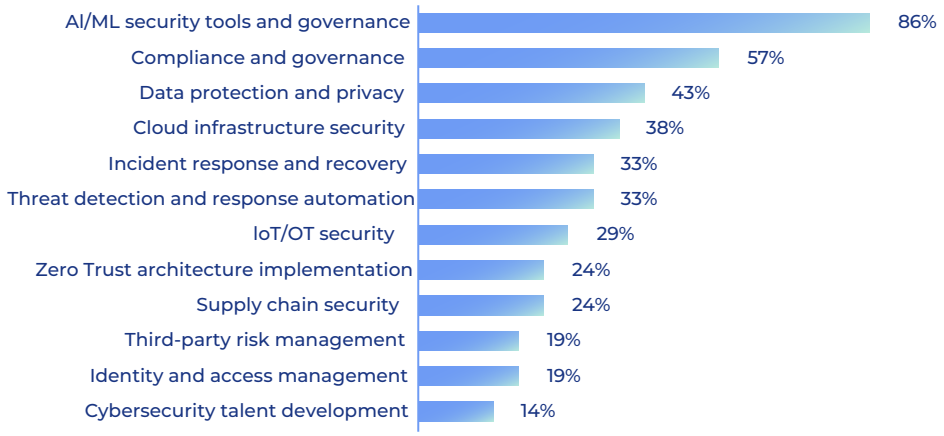
Stability on the Surface, Tension Underneath

Any analysis of cybersecurity strategy must begin with resources. When asked about budget trends over the past 24 months, **57% of organizations reported stable budgets**, a finding that, at first glance, might suggest a sector in equilibrium. Yet stability is not the same as sufficiency, and the data that follows reveals a profound gap between what organizations want to achieve and what their current resource base can realistically support.



How has your cybersecurity budget changed in the past 24 months?

This tension becomes immediately apparent when examining future investment intentions. A striking **86% of organizations plan to increase investment in AI/ML security tools**, making it the dominant priority for the period ahead. This is followed by Compliance and governance, Data Protection and Privacy and Cloud Infrastructure Security.



Which cybersecurity domains will require the highest additional investment in your organization over the next 24 months?

The paradox is stark: if budgets have been largely stable, where will the funding for these ambitious initiatives come from? The answer, almost inevitably, is **reallocation**, and the data reveals exactly where organizations are choosing not to invest. **Cybersecurity talent development ranks dead last among future investment priorities at just 14%**. This single data point, perhaps more than any other in the survey, encapsulates the strategic contradiction at the heart of the sector's current trajectory. Organizations are racing toward sophisticated, AI-driven security architectures while systematically starving the human capital development that would make those architectures effective.

The implications of this choice are not immediately visible, **talent gaps do not trigger alerts or generate incident reports**. But they accumulate silently, eroding the organization's ability to evaluate vendors effectively, implement tools successfully, interpret security data accurately, and respond to incidents decisively.

Current Investment Priorities: The Present-Day Landscape

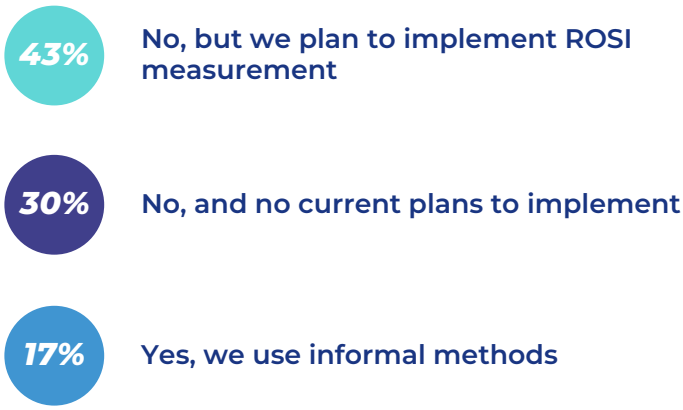
Understanding where organizations are investing today provides essential context for interpreting their future ambitions.

Please rank the following cybersecurity domains by current investment level in the past 24 months

The concentration of investment at the top of this list, in monitoring, detection, and response, reflects an industry that is primarily **oriented toward *reacting* to threats rather than *preventing* them**. The domains that rank lowest (vulnerability management, and application security) are precisely the foundational capabilities that would reduce the volume and severity of threats that monitoring and detection systems must handle. This inversion of priorities, as we will see throughout this chapter, is a recurring theme.

The Measurement Problem: Flying Without Instruments

Before any investment can be made, it must be justified. And the survey reveals a striking truth about how cybersecurity spending is validated within organizations: **73% of organizations do not formally calculate Return on Security Investment (ROSI)**. Of these, 43% acknowledge they plan to implement such measurement but have not yet done so, while 30% have no plans to measure ROSI at all.



Does your organization formally calculate Return on Security Investment (ROSI) for cybersecurity initiatives?

This is not merely an accounting gap, it is a strategic one. Without the ability to demonstrate the financial value of security investments, cybersecurity leaders are left without their most powerful tool for making the case to senior management and boards. The consequences are predictable and visible in the data: **in the absence of value-based justification, organizations default to external pressure as their primary rationale.**

Business Impact Analysis: The Dominant but Borrowed Framework

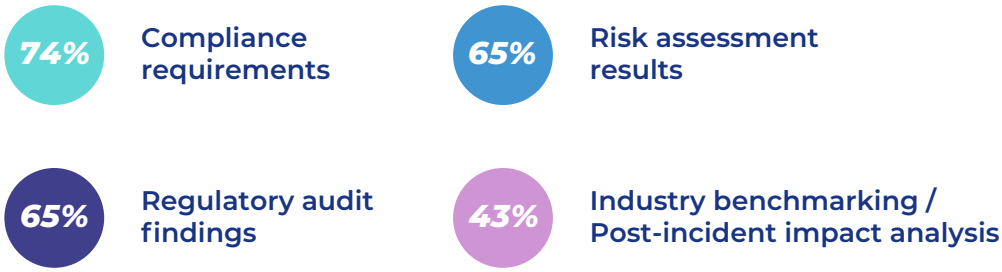
Among the minority of organizations that do measure ROSI, a clear pattern emerges. When asked which methodologies they use, **50% employ Business Impact Analysis (BIA)**, making it the most popular approach by a significant margin.

If you are using ROSI, which methodologies does your organization use for ROSI calculation?

The dominance of BIA is significant and revealing. BIA is fundamentally a **business continuity and disaster recovery tool**, designed to assess the financial impact of operational disruptions. Its adoption as the primary ROSI methodology suggests that organizations are **borrowing frameworks from adjacent disciplines** rather than building dedicated security measurement capabilities. This is a pragmatic response to a real gap, but it also indicates that security ROI measurement remains an immature practice in the Hong Kong market.

Compliance as the Default Justification

When asked how they justify cybersecurity investments to senior leadership, the data is unambiguous: Compliance dominates by a significant margin.



How does your organization typically justify cybersecurity investments to senior management?

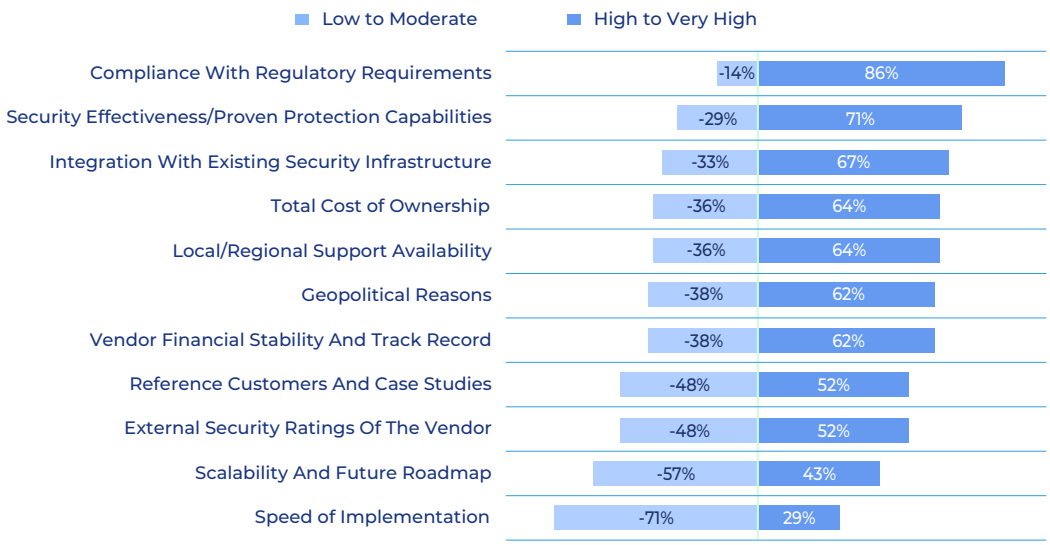
This is not inherently problematic, compliance is real, regulatory requirements are binding, and audit findings are material. But the data reveals a reactive posture rather than a proactive, value-driven one. **Security spending becomes something organizations do *because they must*, rather than something they do *because they can demonstrate it works*.**

This **compliance-first mindset** has cascading effects throughout the organization. It shapes not only how investments are justified internally, but also how vendors are selected, how priorities are set, and ultimately, how the entire security function is perceived by the broader

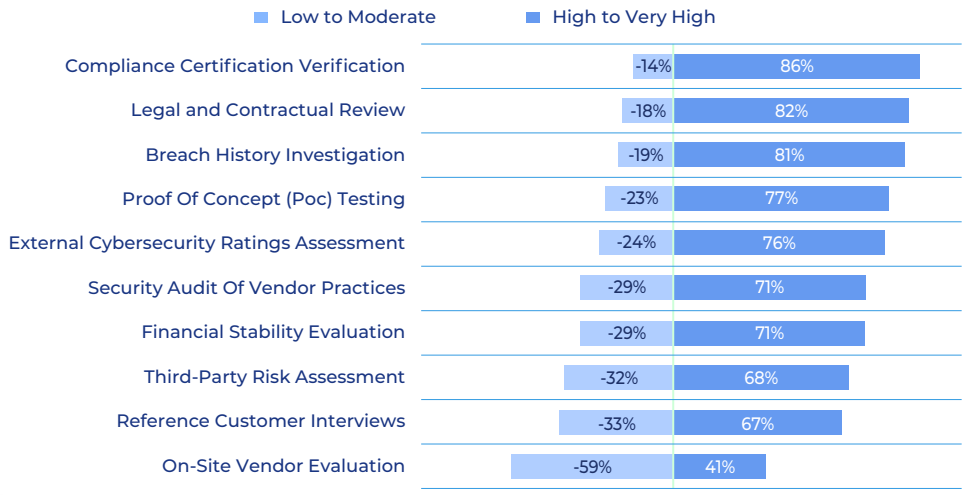
business. When cybersecurity is framed primarily as a compliance exercise, **it struggles to claim the strategic seat at the table** that the current threat environment demands. The CISO becomes a compliance officer rather than a strategic risk advisor. Security investments become line items to be minimized rather than capabilities to be optimized. And the organization's actual security posture, its real-world resilience against real-world threats, becomes secondary to its ability to pass the next audit.

Vendor Selection: Rigorous Process, Persistent Frustration

The compliance-first mindset previously identified manifests most clearly in how organizations select their cybersecurity vendors. When evaluating potential partners, the criteria are extensive and rigorous.



If the choice is BUY over BUILD, please rank the following criteria by importance in your cybersecurity vendor selection process?



Please rank the following due diligence activities your organization performs during vendor evaluation by importance.

This is a picture of organizations that apply considerable rigor to their vendor selection processes. **The due diligence is thorough, multi-layered, and defensible.** The consistency between selection criteria and due diligence activities is itself notable, organizations are not just saying they care about compliance and breach history; they are actually conducting the activities that verify these dimensions.

67% 1

- Geopolitical considerations and data sovereignty
- AI/ML integration capabilities

67% 2

- Supply chain security transparency
- Real-time threat intelligence integration

33% 3

- Zero Trust framework support
- Regulatory compliance automation
- Quantum-ready encryption capabilities

Considering the evolving threat landscape, which factors will become most important in cybersecurity vendor selection over the next 3-5 years?

The prominence of **geopolitical considerations** at 67% deserves particular attention. This is not a standard compliance checkbox, it reflects a sophisticated awareness of Hong Kong's unique position in the global geopolitical landscape, and the growing concern about where data is stored, who has access to it, and whether vendors have dependencies on jurisdictions that may be adversarial or unpredictable. For a city that sits at the intersection of Chinese and international regulatory frameworks, this concern is both rational and strategically important.

The Persistent Gap: When Rigor isn't Enough

And yet, despite this thoroughness, the outcomes are not entirely satisfying. **The gap between vendor marketing and actual capabilities ranks as a top-three challenge for 32% of respondents**, a finding that suggests the current evaluation framework, however detailed, is not fully equipped to cut through the noise of a crowded and complex marketplace. Equally, **32% cite the proliferation of vendors and solution complexity** as a significant challenge, reflecting a market that has become almost overwhelming in its breadth.

- 86% Budget constraints and cost justification
- 59% Skills shortage in cybersecurity talent
- 32% Vendor marketing vs. actual capabilities gap
- 32% Unclear or changing regulatory requirements
- 32% Proliferation of vendors and solution complexity
- 27% Measuring effectiveness and ROI
- 23% Executive understanding of cybersecurity needs
- 23% Overlapping features with other solutions
- 23% Rapid pace of technology change
- 23% Difficulty integrating with existing infrastructure

What are the primary challenges your organization faces in selecting cybersecurity solutions?

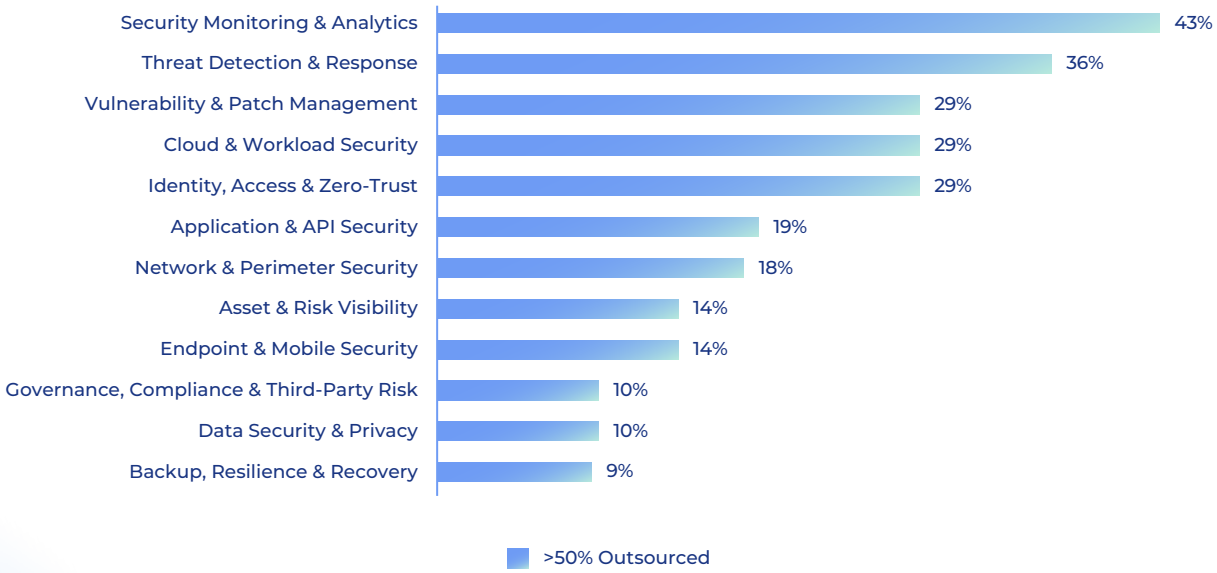
What emerges is a picture of organizations that are doing many of the right things in vendor evaluation, but within **a framework that is shaped more by compliance imperatives and risk mitigation than by a clear-eyed assessment** of what will actually make them more secure or operationally effective. The process is rigorous but the outcomes remain uncertain.

The vendors that pass the compliance and legal gauntlet are not necessarily the vendors that will integrate smoothly, perform effectively, or deliver measurable security value. Compliance certifications tell you that a vendor has met a defined standard at a point in time, they do not tell you whether the vendor's technology will work in your specific environment, whether their support team will be responsive when you need them, or whether their roadmap aligns with your evolving security needs. **The evaluation framework is optimized for defensibility rather than effectiveness**, and the gap between vendor promises and delivered capabilities is the predictable result.

The dominance of **cost as the #1 challenge** reinforces the budget tension identified earlier. Organizations are not just constrained by stable budgets, they are actively feeling the pressure of high costs as a barrier to effective vendor selection and solution adoption. When cost is the primary filter, the evaluation process becomes distorted: organizations may select vendors that are affordable rather than optimal, or defer investments in critical capabilities because the price point is prohibitive.

The Build vs. Buy Dilemma, and the GRC Paradox

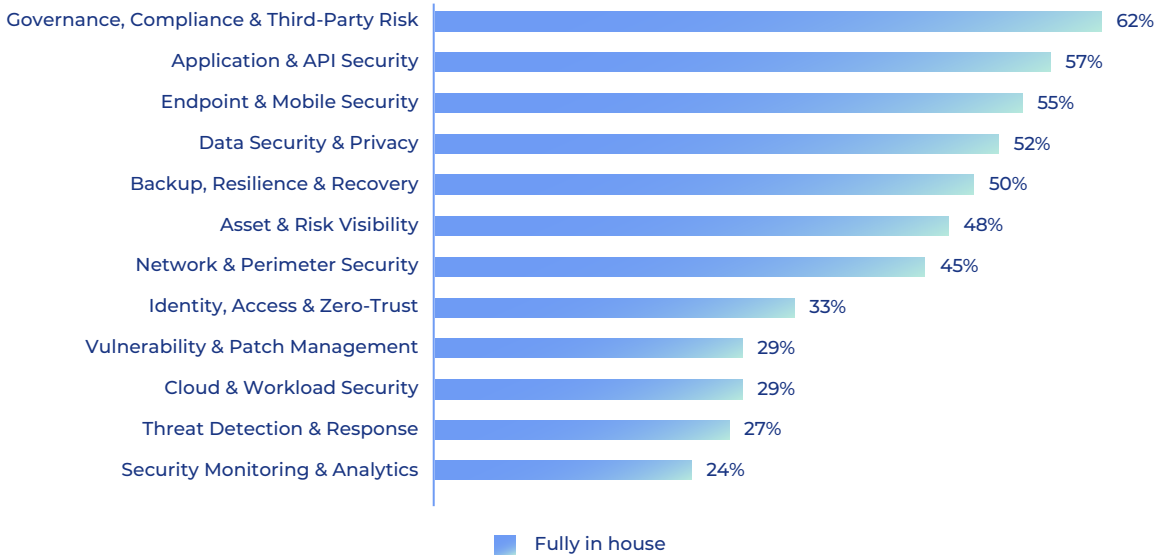
One of the most revealing questions in the survey asks how organizations distribute their cybersecurity work between in-house teams and external vendors. The answers reveal a clear pattern, but with one striking exception.



For each cybersecurity domain below, please indicate your organization's outsourcing level to third party solutions and third-party services?

The Outsourcing Logic: Rational Under Constraint

According to the survey, the most heavily outsourced domains are Security Monitoring & Analytics, Threat Detection & Response, Vulnerability & Patch Management. These are the domains that are most operationally intensive, require 24/7 coverage, and demand specialized expertise. Organizations are making a rational choice: **outsource the work that is hardest to staff and most expensive to run in-house**. Security monitoring, in particular, requires continuous coverage across all hours and time zones, a staffing challenge that is simply beyond the reach of most organizations operating in a constrained talent market.



For each cybersecurity domain below, please indicate your organization's outsourcing level to third party solutions and third-party services?

On the other hand, among the domains that most heavily kept in house, GRC finding is particularly striking. Organizations are **guarding their governance function jealously**, keeping it entirely in-house at rates that exceed even application security. This likely reflects several factors: regulatory sensitivity, data confidentiality concerns, the belief that compliance is a core competency that cannot be delegated, and the reality that **GRC decisions have legal and reputational implications** that organizations are unwilling to outsource.

There is also a cultural dimension to this finding. In Hong Kong's regulatory environment, where relationships with regulators matter, where audit findings have direct consequences, and where compliance failures can result in penalties, the idea of delegating governance to an external party feels genuinely risky. The in-house GRC team is not just a functional unit; it is the organization's primary interface with the regulatory world, and that interface is too important to entrust to a third party.

The Past: A Pattern of Systematic Underinvestment

The current investment data tells a clear story: **GRC ranks 7th out of 12 domains** in current investment levels, not at the bottom, but notably behind the top-funded areas. Security monitoring, endpoint security, and threat detection command the

highest investment, reflecting the sector's continued prioritization of detection, response, and perimeter defense. By contrast, **governance and compliance have been treated as a cost to be minimized rather than a capability to be built**, leaving GRC in the lower half of the investment landscape despite its foundational role.

This underinvestment has been sustained by a particular organizational logic: **62% of organizations currently manage GRC fully in-house, with a further 24% using a hybrid model. Only 14% have outsourced GRC to a managed service provider.** The rationale for keeping GRC internal is understandable: compliance and risk management touch the most sensitive aspects of organizational operations, and there is a genuine concern about entrusting that function to external parties. Regulatory requirements in Hong Kong, particularly those with cross-border implications under China's CSL, DSL, and PIPL, reinforce this instinct toward internalization.

But the combination of in-house management and chronic underinvestment has created what might be called the GRC Paradox: organizations treat GRC as too important to outsource, yet too low a priority to fund adequately. The result is **a compliance function that is simultaneously over-relied upon and under-resourced**, staffed by stretched teams managing complex regulatory obligations with inadequate tools, manual processes, and limited analytical capability.

The consequences of this paradox are visible throughout the survey data. The inability to measure security investment returns (where 73% cannot demonstrate ROSI) is partly a governance failure, without robust risk frameworks and measurement infrastructure, security spending cannot be connected to business outcomes. The integration challenges, (where 50% cite integration difficulties as a top operational barrier) are partly a GRC failure, without strong governance processes, technology deployments lack the organizational scaffolding needed to succeed. And the compliance-first investment justification identified, while effective in the short term, is a **symptom of a governance function that has been reduced to a reactive, audit-driven activity rather than a strategic, value-creating one**.

The Future: A Decisive Course Correction

Here is where the narrative must shift, because the forward-looking data tells a fundamentally different story.

Compliance & Governance ranks #2 among all future investment priorities, with 57% of organizations planning to increase investment, second only to AI/ML at 86%, and ahead of Data Protection and Privacy (43%), Cloud Infrastructure Security (38%), and every other domain in the survey. This is the single largest gap between current investment and future intent of any domain in the survey, a gap of 21 percentage points between where GRC investment stands today (36%) and where organizations intend to take it.

This is not a marginal adjustment. It is a sector-wide recognition that the GRC Paradox has become unsustainable, and that the time has come to address it with genuine investment. Several forces are driving this shift:

1. Regulatory pressure is intensifying and becoming unavoidable. The Hong Kong regulatory landscape is growing more complex and more demanding. The HKMA's CFI 2.0 framework, the SFC's evolving cybersecurity requirements, the anticipated PDPO amendments, and the extraterritorial reach of China's CSL, DSL, and PIPL are creating a compliance burden that manual, under-resourced in-house teams can no longer manage effectively. Organizations are recognizing that the cost of non-compliance, in fines, reputational damage, and regulatory scrutiny, now exceeds the cost of proper GRC investment.

2. The in-house model is being modernized, not abandoned. The planned increase in GRC investment does not signal a retreat from the in-house model. Rather, it signals a **modernization** of it. Organizations that have historically managed GRC manually are preparing to invest in third-party GRC platforms, compliance automation tools, and risk management solutions that will augment and enhance their in-house capabilities. The 62% who currently manage GRC fully in-house, are not planning to outsource, **they are planning to equip their internal teams with the tools they have long lacked.**
This is a significant and positive development. It suggests that the GRC function is about to undergo a structural transformation, from a manual, reactive compliance activity to a technology-enabled, data-driven governance capability. The vendors best positioned to capture this demand will be those offering solutions tailored to Hong Kong's specific regulatory environment, with strong data residency guarantees and the ability to integrate with existing security infrastructure.

3. The convergence with AI creates a transformative opportunity. The 57% planning to increase GRC investment and the 86% planning to increase AI/ML investment are not independent trends. They are **converging in the emergence of AI-powered GRC platforms**, tools that offer automated regulatory change monitoring, AI-assisted risk assessment, intelligent compliance gap analysis, and predictive audit readiness capabilities. This convergence has the potential to be genuinely transformative: it could address the measurement gap that currently prevents organizations from demonstrating ROSI, reduce the burden on stretched in-house teams, and create a more dynamic, real-time approach to governance that goes far beyond traditional compliance management.

4. Data sovereignty concerns are accelerating GRC investment. When asked about future vendor selection criteria, **67% of**

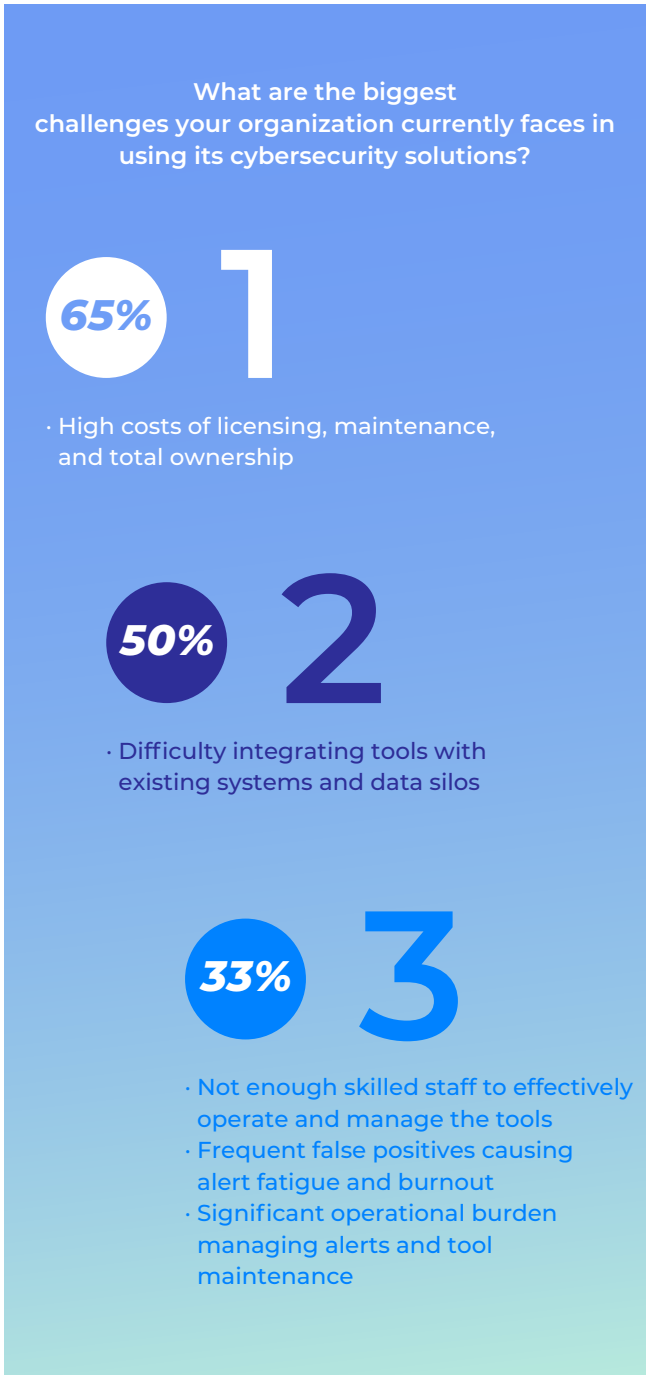
organizations rate geopolitical considerations and data sovereignty as High to Very High priority, making it the #1 future vendor selection factor. GRC platforms, which by their nature contain the most sensitive organizational data (risk assessments, compliance gaps, audit findings, third-party risk profiles) are at the center of this concern. The planned investment in GRC tools will therefore be shaped not just by functional capability, but by the ability of vendors to offer genuine data residency guarantees and architectural independence from geopolitically sensitive supply chains.

The Talent Crisis: Acknowledged but Underfunded

No finding in the survey is more troubling in its implications than the treatment of cybersecurity talent. The data tells **a story of a problem that is clearly recognized but systematically under-addressed**, and the consequences of this gap ripple through virtually every other dimension of the survey.

The Scale of the Challenge

Skilled staff shortage appears as the #3 operational challenge, tied with alert fatigue, both of which are symptoms of the same underlying problem: organizations have more tools and more alerts than they have people to manage them effectively. **The integration challenge at #2 (50%)** is also, in significant part, a talent problem, integrating tools with existing systems requires skilled engineers who understand both the tools and the infrastructure, and those engineers are precisely the people organizations are struggling to recruit and retain.



Across multiple questions and multiple framings, the message is consistent: organizations know they do not have enough skilled people, and they know this is hurting them. The talent challenge also intersects with the regulatory environment in ways that compound the difficulty. **32% of respondents cite unclear or changing regulatory**

requirements as a significant challenge, and navigating regulatory complexity is itself a specialized skill that requires experienced professionals. When the regulatory landscape is shifting and the talent pool is thin, organizations face a compounding challenge that no amount of technology investment can fully resolve.

The Investment Paradox: Acknowledging the Problem While Underfunding the Solution

And yet, as noted previously, **talent development receives the lowest allocation of future investment at just 14%**. This is not an oversight, it is a choice, and it is a choice that creates a self-perpetuating cycle:

1. **Without investment in talent development,** skills gaps persist and widen.
2. **Persistent skills gaps** make it harder to evaluate vendors effectively, implement new tools successfully, and measure security outcomes rigorously.
3. **The inability to measure outcomes** makes it harder to justify investment in talent development, because the value of skilled people, like the value of GRC, is largely invisible until something goes wrong.
4. **And so the cycle continues,** with each iteration leaving the organization slightly more dependent on technology and slightly less capable of using it effectively.

This cycle is particularly damaging because it prevents organizations from breaking out of the compliance-first mindset previously identified. Skilled security professionals are the ones most likely to push for value-based justification of investments, to challenge vendor claims, and to build measurement frameworks. Without them, organizations remain trapped in a reactive, compliance-driven posture, doing what they must rather than what they should.

The 14% figure also needs to be understood in the context of what talent development actually requires. It is not just about training courses or certification programmes, though those matter. **It is about creating career pathways that retain experienced professionals**, building mentoring structures that develop junior talent, establishing communities of practice that share knowledge across teams, and investing in the organizational culture that makes cybersecurity a rewarding and sustainable career. These are not expensive initiatives in absolute terms, but they require sustained attention and deliberate investment, precisely the kind of investment that gets crowded out when budgets are stable and the pressure to invest in technology is overwhelming.

Alert Fatigue: The Human Cost of Underinvestment

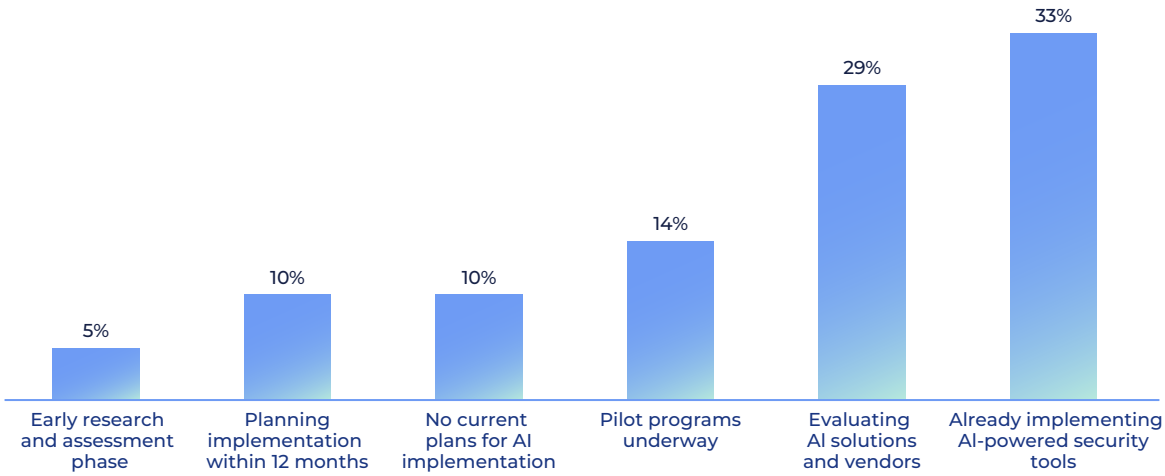
The talent challenge also has a human cost that the data hints at but does not fully capture. **33% of organizations report frequent false positives causing alert fatigue and burnout**. This is not just an operational problem, it is a retention problem. Alert fatigue is one of the leading causes of burnout in security operations, and burnout is one of the leading causes of talent leaving the industry.

Organizations that cannot manage alert fatigue effectively are not just struggling operationally, they are actively driving away the skilled people they desperately need. The security analyst who spends eight hours a day triaging false positives is not developing the skills, the judgment, or the professional satisfaction that would keep them in the role. They are burning out, and when they leave, they take with them institutional knowledge, contextual understanding, and hard-won expertise that cannot be easily replaced.

The irony is that **alert fatigue is itself a symptom of underinvestment in talent.** Organizations that have skilled, experienced security teams are better able to tune their detection systems, reduce false positive rates, and build the operational processe sthat make alert management sustainable. Organizations that are perpetually under-staffed and under-skilled cannot invest the time and expertise required to optimize their detection systems, and so the false positives accumulate, the fatigue deepens, and the talent drain accelerates.

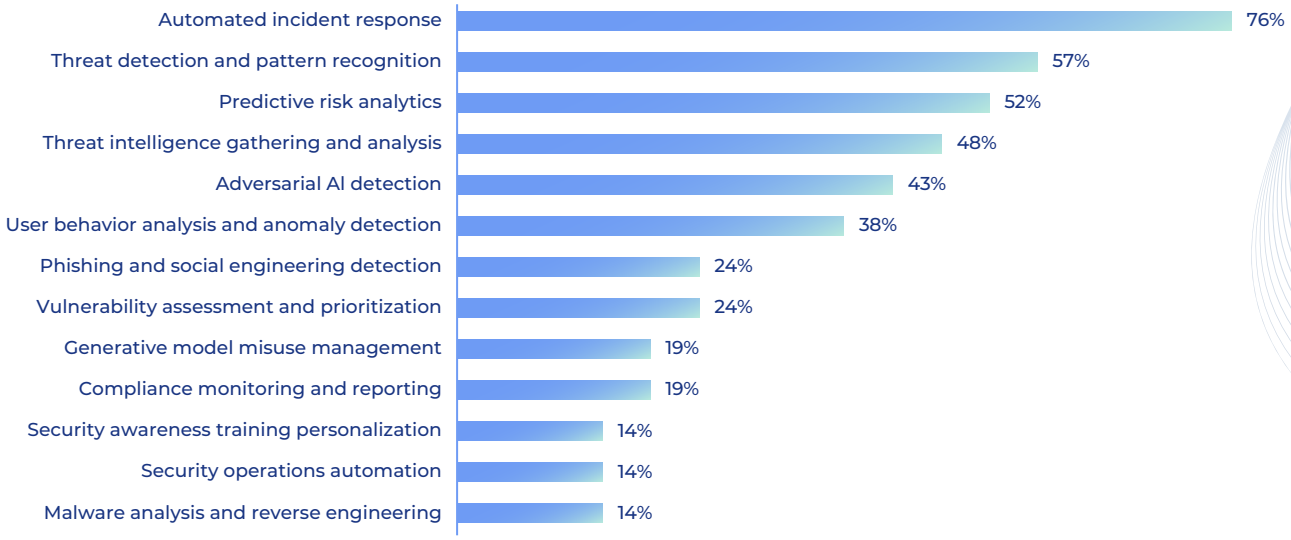
The AI Frontier: Ambition meets Reality

The survey's forward-looking data reveals an industry in the early stages of a significant technological transition. **62% of organizations are already implementing or evaluating AI-powered security solutions**, with 33% actively implementing and 29% in the evaluation phase. Combined with the 86% who plan to increase AI/ML investment, this represents a near-universal orientation toward AI as the defining technology of the next phase of cybersecurity.



What is your organization's current status regarding AI implementation in cybersecurity?

The enthusiasm is understandable. AI-powered security tools offer genuine promise: faster threat detection, more sophisticated behavioral analysis, automated response capabilities, and the ability to process volumes of data that no human team could manage. In a threat environment that is growing in both sophistication and scale, **AI represents a meaningful force multiplier**, and for organizations struggling with talent scarcity and alert fatigue, the appeal of automation is particularly strong.



Where do you believe AI will contribute most significantly to cybersecurity within your organization?

The AI Use Cases: Where Organizations See the Value

These are sophisticated use cases that require not just AI capability but deep integration with existing security infrastructure, skilled interpretation of results, and organizational readiness to act on AI-generated recommendations. The fact that **76% plan to use AI for automated incident response** is particularly telling, it suggests organizations are betting on AI to solve the staffing problem identified. If AI can automate the response to common incidents, the argument goes, then the skills gap becomes less critical.

This is a plausible hypothesis, but it rests on several assumptions that the survey data calls into question. Automated incident response requires well-defined playbooks, clean and integrated data, and a security environment that is sufficiently well-understood to allow automation without unacceptable risk of false positives or unintended consequences. These are precisely the foundational capabilities that organizations are currently under-investing in.

The use case for **predictive risk analytics (52%)** is similarly ambitious. Predictive analytics requires high-quality historical data, robust data infrastructure, and skilled analysts who can interpret and act on predictions. Organizations that currently struggle to measure their existing security investments are unlikely to have the data infrastructure and analytical capability required to make predictive analytics work effectively.

The Readiness Gap: Ambition Without Foundation

The survey data reveals the gap between ambition and readiness with uncomfortable clarity. Recall from the previous paragraph that the top operational challenges organizations face today are **high costs, integration difficulties, skills gaps and alert fatigue**.

These are precisely the barriers that will determine whether AI investments succeed or fail. **AI security tools are expensive to acquire and maintain**, they will intensify the cost pressure that is already the #1 operational challenge. They are complex to integrate

with existing infrastructure, they will add to the integration difficulties that are already the #2 challenge. And they require skilled professionals to configure, monitor, and interpret, the very professionals that organizations are struggling to recruit, retain, and develop.

There is also a deeper question embedded in the data: if most organizations struggle with measuring the return on their existing security investments, **how will they evaluate the effectiveness of their AI deployments?** Without robust measurement frameworks, the risk is that AI becomes the latest iteration of a familiar pattern, significant investment, uncertain outcomes, and justification driven by compliance and peer pressure rather than demonstrated value.

Conclusions: Six Tensions, One Strategic Moment

This analysis has traced six interconnected tensions that define the current state of cybersecurity investment and strategy in Hong Kong's market. Each tension reflects **a genuine strategic challenge and a gap between where organizations are and where they need to be.** Taken together, they describe a practice at a genuine inflection point: one that has built significant capability in some areas while leaving critical gaps in others, and that is now facing a set of investment decisions that will determine its trajectory for the next decade.

The Six Tensions: A Final Synthesis

Tension 1: Compliance-Driven Investment vs. Strategic Value Creation: Organizations justify security investment primarily through compliance obligations and risk avoidance, while simultaneously recognizing that they cannot demonstrate the return on that investment, where 73% cannot calculate ROSI. The result is **a sector that spends significantly on security but cannot articulate why specific investments are more valuable than others.** The planned surge in GRC investment offers an opportunity to break this cycle, but only if organizations use GRC platforms to build genuine measurement capability rather than simply automating existing compliance processes.

Tension 2: Advanced Ambition vs. Foundational Gaps: Organizations are planning to invest heavily in AI/ML and GRC platforms in the coming years, yet current investment patterns reveal a persistent underinvestment in foundational capabilities: vulnerability management, application security, and cloud security all rank in the bottom half of current investment priorities (#9, #10, and #11 respectively). The tension is not between future and past, but within the current investment landscape itself: **advanced and emerging capabilities are being prioritized while the underlying security foundations remain underfunded**. The risk is that advanced investments are built on weak foundations, producing sophisticated tools that cannot deliver their full potential because the underlying security infrastructure is inadequate. The organizations that will succeed are those that sequence their investments strategically, closing foundational gaps while building toward advanced capabilities, rather than leapfrogging the foundations entirely.

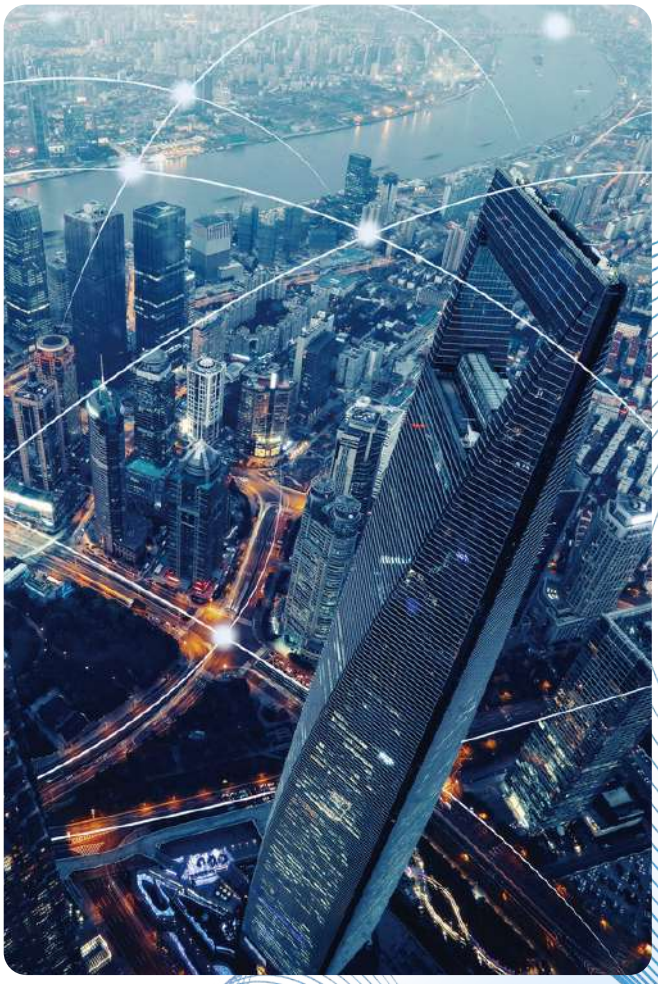
Tension 3: In-House Control vs. Operational Capacity: The preference for in-house management, strongest in GRC (62% fully internal) reflects legitimate concerns about regulatory sensitivity, data confidentiality, and governance accountability. But in-house management without adequate investment produces the **GRC Paradox: functions that are too important to outsource but**

too underfunded to be effective. The planned GRC investment surge is the sector's answer to this paradox: not outsourcing the function, but equipping in-house teams with the tools they need to manage it effectively. This is the right strategic direction, and the execution challenge is ensuring that tool investment is accompanied by talent investment.

Tension 4: Talent Scarcity vs. Technology Ambition: The cybersecurity talent gap is structural and worsening, yet **talent development ranks dead last among future investment priorities at 14%**. Organizations are planning to deploy sophisticated AI-powered security tools and complex GRC platforms while simultaneously under-investing in the people who will implement, operate, and interpret those tools. This is the most dangerous tension in the survey, because it is the one most likely to cause other investments to fail. No technology investment, however well-conceived, can succeed without skilled professionals to make it work.

Tension 5: Integration Complexity vs. Investment Acceleration: 50% of organizations cite integration difficulties as a top operational barrier, yet the planned investment surge (in AI, GRC platforms, cloud security, and zero-trust architecture) will dramatically increase integration complexity. **Organizations are accelerating investment in a context where they are already struggling to integrate their existing technology stack**. The risk is not that the investments are wrong, but that they are being made faster than the organization's integration capability can absorb. Vendors that prioritize integration capability as a first-class feature, and organizations that invest in integration architecture alongside individual technology investments, will be better positioned to realize the value of their planned investments.

Tension 6: Geopolitical Complexity vs. Operational Simplicity: Hong Kong's unique position at the intersection of global and Chinese regulatory frameworks creates a vendor selection challenge that has no simple solution (where 67% rate geopolitical considerations as the #1 future selection criterion). Organizations need **vendors that can operate across multiple jurisdictions**, offer genuine data sovereignty guarantees, and navigate the increasingly complex geopolitical landscape, while also delivering the technical capability, integration support, and talent enablement that operational success requires. This is a demanding set of requirements, and the vendors that can meet all of them will be rare and valuable.



Part 3. Voices from the Ground: Experiences from Cybersecurity professionals

To complement the findings of this research, five Hong Kong-based organizations were invited to share their **firsthand experiences in selecting and deploying cybersecurity solutions**, with a particular focus on tools originating from Mainland China. The organizations operate across different sectors and vary in size and geographic footprint, spanning financial services, multinational corporations, and technology-driven enterprises, yet their journeys reveal a striking degree of convergence around a shared set of challenges and decisions.

Case studies occupy a unique and irreplaceable role in applied research of this kind. Where surveys and market analyses can identify trends at scale, it is the granular, lived experience of practitioners, the procurement decisions made under regulatory pressure, the proof-of-concept failures that reshaped vendor shortlists, the post-deployment surprises that no RFP process could have anticipated, that yields the most actionable insight. By documenting these experiences in structured form and sharing them with the broader cybersecurity community, **this research aims to reduce the knowledge gap that too often forces organizations to learn the same lessons independently**, at significant cost in time, resources, and risk exposure. The practitioners who contributed to these cases did so in the spirit of collective advancement: the belief that the field grows stronger when hard-won experience is made available to those who come after.

Across all five cases, common themes emerge with notable consistency. **Procurement discipline**, the rigorous use of RFI, RFP, and proof-of-concept processes with clearly defined success criteria, repeatedly proved to be the differentiator between well-governed decisions and costly missteps. **Geopolitical awareness** shaped not only vendor selection but architectural design,

with several organizations concluding that a single unified global security stack is no longer a realistic ambition across the Greater China region. Vendor maturity emerged as a nuanced consideration: **Chinese solutions consistently demonstrated strengths** in regional regulatory alignment, cost competitiveness, and vendor responsiveness, while in some areas, such as reporting maturity, multilingual support, and feature depth, they reflected a different stage of product development compared to established international alternatives. And throughout, organizations grappled with the enduring tension between cost efficiency and operational excellence, a tension that rarely resolves cleanly in either direction.

This chapter does not aim to reproduce each case study in full detail. Rather, it **distills the most significant lessons learned and highlights the patterns that cut across all five experiences**, offering practical guidance for cybersecurity leaders navigating similar decisions in the region. The goal is not to prescribe a single path, but to illuminate the terrain, so that those who follow may make better-informed choices, with a clearer understanding of both the opportunities and the trade-offs that define this rapidly evolving landscape.

The Five Cases at a Glance

Case 1: Closing a Regulatory Gap: DNS Security in the Banking Sector

The first case examines how a mid-sized Hong Kong financial institution responded to a **regulatory wake-up call**. During an iCAST exercise conducted by the Hong Kong Monetary Authority, the organization discovered a significant gap in its DNS security posture, specifically, its inability to detect and prevent command and control communications and data exfiltration through DNS tunneling. Rather than rushing to a solution, the team ran a **structured evaluation** that included a broad market scan, onsite proof-of-concept testing, and a formal tendering process, deliberately comparing both Western and Mainland Chinese vendors. They ultimately selected a Chinese DNS security provider, deploying a cloud-based DNS query lookup approach to meet their immediate regulatory obligations within timeline and cost constraints. Post-deployment, the organization encountered operational challenges around change management and the limitations of signature-based detection for more sophisticated threats, lessons that prompted the security team to plan a longer-term migration toward a more comprehensive DDI (DNS, DHCP, and IP Address Management) architecture.

Case 2: The Collaboration Platform Dilemma: When Cost Savings Meet Hidden Complexity

The second case involves the Head of Information Security at a large Hong Kong-based multinational, who led a multi-month feasibility study into replacing Microsoft Office 365 with a Chinese collaboration platform. The initial motivation was straightforward: the Chinese alternative offered an **estimated 40–50% reduction in licensing costs**, and there was a strategic interest in reducing dependence on a single Western vendor. The evaluation quickly revealed, however, that cost was not the real issue. The organization had accumulated years of deeply embedded Office 365 dependencies, Teams conversations representing roughly 40% of internal communications, SharePoint sites hosting regulated documents, and complex encryption policies and sensitivity labels that could not be cleanly migrated. The evaluation also surfaced a fundamental difference in security philosophy: where Western platforms are built around the concept of the managed device, Chinese platforms tend to concentrate security controls within powerful application-layer environments, with a weaker equivalent to **Mobile Device Management** as understood in Western enterprises. **Despite the compelling financial case, the organization chose to remain with Office 365,** concluding that the migration risk, legacy integration complexity, and long-term operational friction outweighed the savings.

Case 3: Disruption as Catalyst: Rebuilding Endpoint Security After CrowdStrike

The third case describes a Hong Kong-based multinational that was forced into a comprehensive re-evaluation of its endpoint security architecture following the widely publicized **CrowdStrike** update incident of July 2024, in which a faulty content update caused widespread system failures across millions of Windows devices globally. The organization had already been experiencing integration friction between CrowdStrike and its existing SASE environment, and the incident served as the catalyst for a broader strategic review. Following a formal evaluation process, including RFI, RFP, cross-functional stakeholder alignment, and a proof-of-concept phase, the organization selected a leading Endpoint Detection & Response Platform and Integrated XDR Platform as its replacement platform. The decision was driven by the vendor's deep integration with the organization's existing Cloud & Infrastructure environment, compelling total cost of ownership enabled by the existing Enterprise Licensing Agreement, and the platform's ability to address alert correlation across the full security infrastructure. For its Mainland China operations, **the organization adopted a hybrid approach, deploying local Chinese solutions to meet regional regulatory and market requirements.**

Case 4: Best-of-Breed in Practice: Combining Western and Chinese Vendors for ASM and NDR

The fourth case details the deployment of a combined Attack Surface Management (ASM) and Network Detection & Response (NDR) capability at a large Hong Kong-based organization. Faced with growing alert fatigue, unmonitored external assets, and the need to reduce mean time to detect and respond, the organization deliberately adopted **a best-of-breed, multi-vendor strategy** rather than relying on a single integrated platform. **A Western vendor was selected for ASM**, responsible for external asset discovery, continuous monitoring, data leak detection, and third-party risk management; **a Mainland Chinese vendor was selected for NDR**, providing deep network visibility and threat detection enriched by contextual threat intelligence. Both vendors were evaluated through a rigorous process that included structured RFP scoring, strict proof-of-concept success thresholds, covering detection precision, false-positive rates, and discovery coverage, and full security and legal due diligence. The case demonstrates that multi-vendor architectures, while operationally more demanding, can deliver superior outcomes when integration with existing SIEM and SOAR platforms is treated as a first-order requirement from the outset, rather than an afterthought.

Case 5: Navigating Regulatory Divergence: Parallel Security Architectures Across Greater China

The fifth case covers a long-term **SASE and Zero Trust transformation** being rolled out across Hong Kong, Mainland China, and Taiwan by a multinational organization with significant operations across all three markets. From the outset, the initiative was constrained by a fundamental regulatory and political reality: a single unified solution could not be deployed across all three jurisdictions. **Mainland China's data localization requirements, restrictions on certain foreign technology vendors, and divergent compliance obligations under frameworks such as PIPL made a parallel architecture unavoidable.** The organization therefore designed and operates two distinct SASE environments, one for Mainland China, using locally compliant solutions, and one for Hong Kong and Taiwan, using an international platform. In parallel, the organization undertook a regional DLP transition along identical lines, replacing a single global tool with two regional solutions. The Chinese DLP vendor offered meaningful advantages, PIPL-aligned rule sets, competitive pricing, and direct access to senior leadership for rapid escalation and roadmap influence, but also exhibited limitations in reporting maturity, multilingual support, and feature depth compared to international alternatives. The case illustrates with particular clarity the growing reality for any multinational operating across the Greater China region: **the aspiration of a single, unified global security stack is increasingly unachievable**, and the ability to design, govern, and operate parallel technology environments is rapidly becoming a core competency in its own right.

Cross-Cutting Themes and Lessons Learned

Structured Procurement is Non-Negotiable

Across all five cases, the organizations that achieved the best outcomes were those that invested in a **rigorous, formal evaluation process** before committing to a solution. This consistently included requirements definition and gap analysis, market scanning and vendor shortlisting, Proof of Concept (POC) or Proof of Value (POV) testing with pre-defined success criteria, structured RFP processes with scoring methodologies, cross-functional stakeholder involvement, spanning Security, IT, Legal, Finance, and Procurement, and Total Cost of Ownership (TCO) analysis that went beyond licensing fees to include implementation, support, and potential migration costs.

Organizations that bypassed or compressed these steps, particularly those where adoption was driven top-down without sufficient technical due diligence, frequently encountered avoidable complications during deployment. The lesson is clear: **the time invested in structured evaluation pays dividends in reduced operational friction and more defensible investment decisions**.

POC Testing Must Reflect Real-World Complexity

A recurring lesson across the cases is that POC testing, while essential, must be designed to reflect the full complexity of the production environment. In Case Study 3, the initial three-month POC proved insufficient to surface integration challenges that only emerged at scale. In Case Study 4, the organization deliberately set strict success thresholds during the POC phase, including detection precision and false-positive rates, which proved critical to long-term operational confidence.

Best practice, as evidenced across these cases, involves **testing across the full range of deployment scenarios**, including multi-cloud, on-premises, and hybrid configurations, and involving frontline security analysts and end-users, not just technical architects, in the evaluation process.

Geopolitical Risk Has Become a Core Procurement Criterion

Perhaps the most significant and consistent theme across all five cases is the growing weight of geopolitical considerations in technology procurement decisions. This manifests in two distinct but related ways.

First, organizations are **increasingly scrutinizing the national origin of their vendors**, not only Chinese vendors, but also American ones, and assessing the risk of a vendor being sanctioned, banned, or withdrawing from the market over a multi-year horizon. This concern is particularly acute for long-term investments and for organizations operating in politically sensitive environments.

Second, and more structurally, the **regulatory divergence between Mainland China**

and the rest of the region is forcing organizations to abandon the ambition of a single, unified global technology stack. Cases 3, 4, and 5 all illustrate this dynamic explicitly: organizations are adopting **hybrid architectures**, deploying Chinese solutions within Mainland China and international solutions elsewhere, not because of technical preference, but because of regulatory and political necessity. This **dual-system model** introduces persistent complexity: fragmented visibility, duplicated vendor management, and heterogeneous governance frameworks. It is, however, increasingly the pragmatic reality for any organization with meaningful operations across the Greater China region.

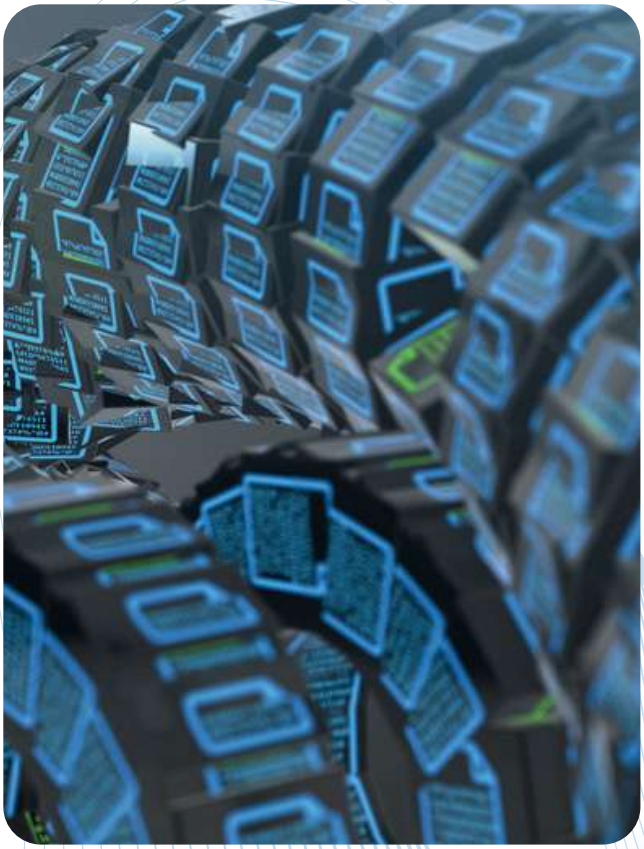
Chinese and Western Solutions Operate on Different Maturity Curves and Different Assumptions

A nuanced but important insight emerging from these cases is that Chinese and Western cybersecurity solutions should not simply be evaluated against the same feature checklist. **They have evolved under different market conditions, regulatory environments, and user expectations,** and this shapes not only what they do, but how they do it.

In the **hardware domain**, Chinese vendors have reached a level of maturity that makes them credible alternatives to Western equivalents, and diversification in this category is increasingly viable. In the **software domain**, the picture is more varied. Several cases noted that Chinese software solutions, particularly in areas such as SASE, DLP, and collaboration platforms, can differ from international alternatives in feature depth, configuration usability, multilingual support, and reporting maturity, though such gaps must be weighed against the meaningful advantages these vendors offer in regional compliance alignment, cost competitiveness, and responsiveness to customer requirements.

Chinese vendors often offer meaningful advantages that are underappreciated in traditional evaluation frameworks: stronger alignment with local regulatory requirements (such as PIPL compliance in DLP solutions), greater commercial flexibility and pricing adaptability, and more direct access to senior vendor leadership, which can accelerate issue resolution and product roadmap influence.

The practical implication is that **evaluation teams must move beyond feature-by-feature comparisons** and instead assess whether a solution adequately addresses the organization's specific risk scenarios, even if the underlying mechanisms differ from what Western tools would employ.



Integration Planning Must Be a First-Order Concern

Across multiple cases, integration emerged as a critical success factor that was either underestimated or addressed too late in the process. In Case Study 3, pre-existing integration friction between CrowdStrike and the SASE solution was a contributing factor in the decision to re-evaluate the entire endpoint security stack. In Case Study 4, the organization deliberately positioned SIEM and SOAR integration as a key success criterion from the outset, and this foresight contributed significantly to the positive operational outcomes achieved.

The lesson is consistent: **integration should not be treated as an implementation detail to be resolved after vendor selection**. It must be evaluated as a primary criterion during the procurement process, with explicit testing of integration capabilities during the POC phase.

Vendor Relationships Matter as Much as Product Capabilities

Several cases highlight that the quality of the vendor relationship, beyond the technical merits of the product, is a significant determinant of long-term success. In Case Study 1, the cultural and operational differences in how the Chinese vendor approached change management required explicit contractual provisions to ensure alignment with banking governance standards. In Case Study 5, the organization valued the direct access to senior leadership within the Chinese DLP vendor, which enabled **faster escalation and greater influence over the product roadmap**.

The ideal vendor relationship, as articulated across these cases, is one built on genuine partnership: regular knowledge sharing, proactive customer enablement, transparent roadmap communication, and a demonstrated willingness to adapt to the client's evolving needs. Organizations should assess these dimensions as carefully as they assess technical capabilities, particularly when committing to relationships expected to span three to five years or more.

Security Strategy Must Evolve Continuously, not Episodically

A final cross-cutting lesson is that **cybersecurity solution selection is not a one-time event**. Several organizations in these case studies found that their initial choices, while appropriate for the immediate challenge, required revisiting as requirements matured, threats evolved, or operational realities became clearer. In Case Study 1, the initial cloud-based DNS query lookup approach was effective in closing the regulatory gap but ultimately insufficient for comprehensive protection, prompting a planned migration to DDI. In Case Study 3, the CrowdStrike incident served as an unplanned but ultimately productive catalyst for a more integrated security architecture.

The implication for cybersecurity leaders is that **technology roadmaps must be treated as living documents**, reviewed at least annually, and informed by continuous feedback from operational teams, threat intelligence, and the evolving regulatory landscape.

Conclusion

The five case studies presented in this chapter collectively illustrate the complexity and nuance of cybersecurity solution selection in Hong Kong's unique operating environment. They demonstrate that **successful procurement requires far more than technical evaluation**: it demands geopolitical awareness, organizational alignment, rigorous testing discipline, and a long-term perspective on vendor relationships.

The question of whether to adopt Chinese or Western cybersecurity solutions does not admit a simple answer. The evidence from these cases points instead toward a category-specific, risk-informed approach, one that neither categorically embraces nor rejects solutions based on their origin, but rather **evaluates them honestly against the organization's specific requirements, operational context, and strategic horizon**. For organizations operating across the Greater China region, the ability to manage this complexity with sophistication and pragmatism is rapidly becoming a core competency in its own right.

Part 4. Beyond the Sales Pitch: What the Vendor Accounts Really Tell Us

To complement the practitioner experiences documented in Part 3, six software vendors, spanning Mainland Chinese and Hong Kong-based providers, were invited to share their firsthand perspectives on the Hong Kong cybersecurity market: its opportunities, its structural challenges, and the trends they expect to shape it over the coming years. The vendors represent a deliberately diverse cross-section of the cybersecurity landscape: SOC services and endpoint protection **(Ansen)**, data loss prevention **(Coworkshop)**, log management and SIEM **(LogEase)**, cloud-native security **(Tencent Cloud Security)**, threat intelligence and network detection and response **(ThreatBook)**, and enterprise IT infrastructure and security **(Digital China)**.

Their accounts are candid, commercially grounded, and, taken together, remarkably convergent. Despite operating in different product categories, serving different customer segments, and occupying very different positions in the competitive landscape, all six vendors have navigated a similar set of challenges and arrived at a recognizably similar set of conclusions. That convergence is itself significant: it suggests **that the dynamics shaping the vendor experience in Hong Kong are not idiosyncratic to any single company or category, but rather structural features of the market as a whole**.

Several themes emerge with particular consistency across all six accounts.

The **most persistent challenge is perception**: the difficulty of being evaluated on merit in a market where brand familiarity, geopolitical anxiety, and procurement inertia continue to shape decisions. ThreatBook highlights the stubborn misconception that Chinese solutions are budget alternatives rather than high-end offerings. Digital China goes further, arguing this is partly self-inflicted, as too many Chinese vendors have

competed primarily on price, damaging the credibility of the broader category.

A second theme is the **evolving regulatory and geopolitical environment**, which all six vendors view as a structural tailwind. The PCIO, Hong Kong's digitalization agenda, and growing appetite for supply chain diversification are opening doors previously closed to Chinese vendors, though vendors are clear-eyed that geopolitics may provide an entrance ticket, but quality and local ecosystem support ultimately determine the outcome.

A third theme is the **importance of deployment support, partner capability, and post-sale service** as differentiators that matter as much as product functionality. In a market where references matter enormously, the quality of the implementation experience shapes vendor reputation as much as the product itself.

A fourth theme concerns the **maturity trajectory of the Chinese cybersecurity vendor market**. All six vendors describe rapid maturation over the past decade, while remaining candid about persisting gaps in product maturity, multilingual support, and enterprise-grade organizational processes.

This chapter does not reproduce each vendor interview in full. Rather, **it distils the most significant insights and identifies the common threads that run across all six perspectives**, offering readers a vendor-side complement to the practitioner experiences documented in Part 3. The goal is to help cybersecurity leaders understand not only what vendors are selling, but how they perceive the market, and what strategic bets they are making on the future, insights that can inform more sophisticated vendor selection, relationship management, and long-term partnership decisions.

The Six Vendors at a Glance

The six vendors featured in this chapter were selected to reflect the diversity of the Chinese cybersecurity ecosystem as it engages with the Hong Kong market. They differ in size, ownership structure, product focus, and go-to-market approach, yet, as the rest of this chapter will show, their experiences and observations converge on a remarkably consistent set of themes. Together, **they cover the full breadth of the cybersecurity stack**: from endpoint protection and SOC services, to data loss prevention, log management, cloud-native security, threat intelligence, network detection and response, and enterprise IT infrastructure. Their accounts are drawn from direct commercial experience in Hong Kong and, in several cases, the broader Greater China region.

A Boutique Specialist Built on Offensive Security DNA. Ansen is an internationally oriented Chinese cybersecurity company whose R&D is rooted in China but whose primary markets are overseas, including Hong Kong and Macau. Its portfolio spans SOC services, endpoint protection, sandbox solutions, and security consulting. What sets Ansen apart is the composition of its team: **approximately half of its workforce consists of offensive and defensive security specialists,** giving its products a strong red-team DNA that informs both product design and customer engagements. Its founding team has been working on malware identification since around 2000 and has maintained a long-term partnership with Google VirusTotal, a relationship that speaks to its standing in the global threat research community.

A Hong Kong-Native Approach to Data Loss Prevention. Coworkshop is a Hong Kong-based vendor specializing in data loss prevention. Rather than scanning content for sensitive data, the approach taken by most DLP solutions, **its core differentiator is a proprietary zone-based technology that protects designated storage locations directly.** This design philosophy is deliberately pragmatic: by avoiding content inspection, it reduces false positives and minimizes disruption to business workflows, making it easier for organizations to sustain DLP programmes over time. Its customers are concentrated in government, financial services, NGOs, and manufacturing, sectors where data governance obligations are high and operational continuity is non-negotiable.

A Cost-Effective SIEM Challenger with a Government Reference. LogEase is a Mainland Chinese log management and SIEM platform that has been in operation for approximately eleven years. It positions itself as a technically credible and cost-effective alternative to established Western platforms such as Splunk, targeting enterprise and government customers who face growing log management obligations but are constrained by budget. Its **most significant Hong Kong reference deployment is with the Digital Policy Office**, where it supports log analysis for the "iAM Smart" application, a government digital identity platform used by millions of residents. This deployment has been instrumental in establishing LogEase's credibility in the Hong Kong public sector.

Hyperscale Infrastructure, Locally Delivered. Tencent Cloud Security brings the scale and infrastructure of one of the world's largest technology companies to the Hong Kong cloud security market. **Its competitive strengths lie in Anti-DDoS and anti-bot capabilities** that have been battle-tested at extraordinary scale through WeChat, gaming, and fintech platforms, environments where the volume and sophistication of attacks far exceed what most enterprise security teams encounter. These capabilities are delivered through local Hong Kong data center infrastructure, enabling customers to benefit from hyperscale threat intelligence while meeting data residency requirements. Its customer base in Hong Kong spans financial services, retail, e-commerce, and logistics.

A High-End Threat Intelligence Provider with Global Recognition. ThreatBook is a Chinese cybersecurity vendor specializing in threat intelligence and network detection and response (NDR). It deliberately positions itself at the high end of the market, targeting financial services, government, and critical infrastructure, and competes on analytical depth and detection accuracy rather than price. This positioning received notable external validation in May 2025, when **ThreatBook became the only Chinese company included in Gartner's inaugural Magic Quadrant for NDR**; it has also received Strong Performer recognition in Gartner Peer Insights for three consecutive years.

An Enterprise IT Veteran Navigating the Security Transition. Digital China is a well-established, listed Mainland Chinese IT company with a long history of serving large enterprises and government organizations in Hong Kong and the broader region. Having built its reputation in IT infrastructure, it has in recent years made a deliberate strategic pivot toward cybersecurity, a transition that reflects both market demand and the company's recognition that infrastructure and security can no longer be treated as separate disciplines. Its cybersecurity portfolio today includes Web Application Firewalls, Zero Trust Security Access, API security, and AI-driven security solutions. **It differentiates itself through enterprise-grade quality assurance processes, deep R&D investment, and a commitment to integrating global threat intelligence,** capabilities it has had to communicate carefully in a market where Chinese vendors are often assumed to compete primarily on price.

The Market Through the Vendor's Lens: Perspectives, Perceptions, and the Road Ahead

1. Perception Is the Primary Barrier, Not Technology or Regulation

Perhaps the most striking point of convergence across all six vendor accounts is the **unanimous identification of market perception**, rather than technical capability or regulatory restriction, as the **dominant barrier to adoption** of Chinese cybersecurity solutions in Hong Kong.

Ansen describes the challenge as one of **"preconceived concerns"** among international customers, which it addresses through transparency, international certifications, and demonstrated performance. Coworkshop points to the hesitancy of overseas customers due to **"security concerns and geopolitical perceptions."** LogEase frames the issue as one of brand recognition: Western vendors have historically enjoyed stronger visibility and longer track records, but argues that the underlying capability gap is narrowing. Tencent Cloud Security identifies **"brand trust in a geopolitical context"** as its most significant challenge, noting that procurement decisions can be influenced by geopolitical anxieties even in the absence of any credible technical evidence of risk. ThreatBook highlights the **persistent misconception that Chinese solutions are budget alternatives rather than high-end offerings.** Digital China identifies two specific perception barriers it encountered upon entering Hong Kong: the absence of local reference cases, and the assumption that all Chinese vendors compete primarily on price.

The consistency of this finding across vendors of very different sizes, product categories, and market histories is significant. It suggests that **the perception challenge is structural and sector-wide**, not a reflection of any individual vendor's shortcomings. It also implies that the path to **broader adoption runs primarily through customer education**, successful reference deployments, and transparent compliance engagement, rather than through product improvement alone.

2. Geopolitics is Opening Doors, but Quality Must Walk Through Them

All six vendors acknowledge that the shifting geopolitical environment is creating new commercial opportunities for Chinese cybersecurity providers in Hong Kong. Governments and enterprises are increasingly **seeking heterogeneous technology stacks that reduce dependence on any single country or vendor**. Ansen describes this as the pursuit of "cyber sovereignty." Digital China notes that geopolitical change has given Chinese vendors "an entrance ticket to conversations previously closed."

However, vendors are equally clear that **geopolitics alone is not sufficient to win business**, particularly in the large enterprise and regulated financial services segments. Digital China articulates this most directly: "for large enterprises, quality, reliability, and local ecosystem support ultimately decide the winner, not geopolitics alone." ThreatBook similarly emphasizes that its competitive strategy is built on positioning as a high-end provider, not a geopolitically convenient alternative.

This nuance is important for readers to understand. **The geopolitical tailwind is real and is accelerating market access for Chinese vendors. But it is creating an opportunity, not a guarantee.** Vendors that compete on quality, innovation, and service depth are likely to build durable customer relationships;

those that compete primarily on price or geopolitical alignment risk contributing to the "race-to-the-bottom" dynamic that Digital China explicitly warns against.

3. The "20 Percent" Problem: Differentiation in a Commoditized Market

Several vendors independently converge on a related insight: that cybersecurity products within the same category often **appear highly similar on paper**, making it difficult for buyers to identify the factors that truly matter for their specific environment. Ansen articulates this most vividly, noting that **two vendors in the same category may look "80 percent similar"**, and that its strategy is to **differentiate itself precisely in the remaining 20 percent**, through fast product iteration, continuous in-depth services, and tight alignment with customers' evolving business needs.

This observation has practical implications for procurement teams. It reinforces the case studies' emphasis on rigorous POC testing and real-world evaluation: **the differentiating 20 percent is rarely visible in a feature comparison or a vendor presentation.** It only becomes apparent through hands-on testing in the customer's own environment, against the customer's own threat scenarios and operational constraints.

4. Deployment Support and Partner Capability Are as Important as Product Quality

A recurring theme across the vendor accounts is that the **quality of implementation support** and the **capability of the local partner ecosystem** are as important and determinant of customer success as the technical merits of the product itself.

LogEase's Digital Policy Office deployment illustrates this clearly: the primary challenge was not technical, but **cultural and operational**, bridging differences in working style and communication habits between Mainland Chinese engineers and Hong Kong engineers. Referring to an important client in Macao, Digital China makes the point even more explicitly: "winning the deal was only the beginning; supporting partner capability development proved equally critical to success." The company invested heavily in training and on-site support to enable its local partner to deliver effectively, and has since made partner capability development a central element of its go-to-market strategy.

For buyers, this is a practical procurement lesson: vendor selection should include an assessment not only of the product, but of the **vendor's implementation methodology**, local support infrastructure, and, where the vendor operates through channel partners, the capability and track record of those partners.

5. Regulatory Change is the Most Powerful Market Catalyst

All six vendors identify Hong Kong's evolving regulatory environment as the single most important driver of near-term market demand. The **Protection of Critical Infrastructures (Computer Systems) Ordinance**, which came into force on 1 January 2026, is cited by multiple vendors, including Ansen, ThreatBook, and Digital China, as a landmark development that will compel organizations across eight critical sectors to invest significantly in cybersecurity governance, risk assessment, and incident response capabilities.

Beyond the PCICSO, vendors serving the financial sector point to the HKMA's Cybersecurity Fortification Initiative and the Insurance Authority's Cyber Resilience Assessment Framework as ongoing drivers of demand. ThreatBook's direct experience with an important client illustrates this dynamic directly: the initial motivation for a large-scale NDR deployment across more than fifty locations was C-RAF compliance, and the relationship deepened as the operational value of the solution became evident over time.

The vendor-side perspective on regulation is worth noting: vendors do not merely view regulatory change as a commercial opportunity. Several also observe that stronger regulation would **help address the management mindset barrier that currently slows adoption of preventive security tools**. When data breach penalties are insufficient to create a deterrent effect, organizations may delay investment until after an incident occurs. Stronger regulation changes this calculus.

6. The Chinese Vendor Market is Maturing, but Unevenly

The vendor accounts collectively paint a nuanced picture of the Chinese cybersecurity vendor landscape: one of genuine and rapid capability development, but also of uneven maturity and a risk of **destructive price competition** as more vendors enter international markets.

Ansen and ThreatBook both describe significant investment in R&D, offensive security expertise, and international standards alignment. ThreatBook's Gartner Magic Quadrant inclusion is the most visible external validation of this maturity trajectory. Tencent Cloud Security's Anti-DDoS and anti-bot capabilities, proven at the scale of WeChat and major gaming platforms, represent

a category where Chinese vendors have demonstrably reached world-class levels.

At the same time, Digital China offers a candid assessment of the broader landscape: many Chinese cybersecurity vendors *"possess strong technical know-how but are weak in product management, quality assurance processes, and organizational maturity,"* and many *"operate with a start-up mentality despite their size."* **This forces price-based competition and "involution"**, a race to the bottom that ultimately damages the industry's reputation and sustainability. LogEase similarly warns of the risk of a price war as more Chinese vendors enter the Hong Kong market.

The implication for buyers is consistent with the case studies' findings: Chinese vendors should be evaluated on their specific capabilities, governance maturity, and service depth, not treated as a homogeneous category. The range of maturity within the Chinese vendor landscape is wide, and the differences matter.

7. The Future Belongs to Integrated, AI-Augmented, Locally Adapted Solutions

Looking ahead, all six vendors converge on a broadly consistent vision of where the Hong Kong cybersecurity market is heading over the next three to five years. Several trends are identified consistently:

Regulatory-driven investment will accelerate across all critical sectors, creating sustained demand for security assessments, SOC services, threat intelligence, and compliance management tools.

AI and machine learning will become central to threat detection, response automation, and increasingly to the protection of AI assets themselves. Tencent Cloud Security specifically identifies AI Security Posture Management and LLM-specific Web Application Firewalls as emerging product categories.

Integrated solutions will be preferred over point products. Customers, particularly in regulated sectors, want security embedded into their infrastructure from the outset, not bolted on as an afterthought. This preference for "security by default" is observed consistently by Tencent Cloud Security and Digital China.

Localized, regionally adapted solutions will gain ground, as organizations seek tools that align with the specific regulatory requirements, threat landscapes, and operational contexts of the Greater China region, including China-specific vulnerability databases (CNNVD, CNVD) and threat intelligence relevant to regional attack actors.

Technological decoupling will continue to shape the market, with organizations increasingly managing parallel technologyenvironments for Mainland China and international

operations. Coworkshop explicitlyanticipates that this decoupling will extend beyond vendor brands to underlying operating systems and IT infrastructure, a development that will require cybersecurity vendors to support both traditional international environments and emerging domestic technology ecosystems simultaneously.

Conclusion

The six vendor perspectives documented in this chapter offer a valuable complement to the practitioner experiences of Part 3. Taken together, they confirm that the Hong Kong cybersecurity market is at an inflection point: geopolitical change, regulatory hardening, and rising threat sophistication are simultaneously expanding the opportunity for Chinese vendors and raising the bar for what customers expect from them.

The most important lesson from the vendor side mirrors the most important lesson from the practitioner side: **origin alone, whether Chinese or Western, is neither a sufficient reason to adopt a solution nor a sufficient reason to reject one**. What matters is technical capability, organizational maturity, service depth, regulatory alignment, and the quality of the long-term partnership. Vendors that understand this, and compete accordingly, are well positioned to grow. Those that rely on geopolitical tailwinds or price competition alone are not.

For cybersecurity leaders in Hong Kong, the **expanding vendor landscape is ultimately good news:** it means more choice, more competition on quality, and more solutions adapted to the specific realities of operating at the intersection of East and West. Navigating that landscape with rigor and sophistication remains, as ever, the essential challenge.

Part 5. Lessons Learned from the Field: Practitioners' Wisdom and the Path Forward

What Three Senior Cybersecurity Leaders Teach Us About Navigating the Investment Paradox

Throughout this study, we have examined the cybersecurity investment landscape through the lens of survey data, market analysis, and regulatory trends. We have identified the **Budget-Security Paradox, mapped the GRC automation imperative, and traced the fault lines between AI ambition and operational reality.** But data, however rigorous, captures what organizations do, not what they have learned from doing it.

This final chapter is based on **three practitioner interviews** conducted with Adrian, Marcus, and Philip[17] as part of this research programme, with three senior cybersecurity leaders operating in Hong Kong and the broader APAC region, to distil the lessons that only experience can teach. Their responses, taken together, form a remarkably coherent body of practitioner wisdom: one that both validates the quantitative findings of this study and enriches them with the texture of lived leadership.

The chapter is structured as **a series of lessons learned, each grounded in the interviewees' responses and connected to the broader research findings**. It closes with a forward-looking perspective and a set of practical tools, including a vendor selection checklist, designed to be of direct use to the cybersecurity leader reading this today.

[17] For confidentiality reasons, the real names of the leaders have been anonymized and replaced with pseudonyms.

Lesson 1: The Board Communication Challenge is Real, but it is Solvable

The survey data is unambiguous: budget constraints and the difficulty of justifying cybersecurity investments are the top challenges facing CISOs in the region. At the heart of this challenge lies **a communication problem**, the gap between the technical language of cybersecurity and the financial and strategic language of the boardroom.

All three interviewees acknowledge this gap, but they approach it from meaningfully different positions, and the contrast is instructive.

Adrian offers the most direct and practically actionable insight. Rather than relying solely on dashboards and metrics which, as he notes, senior management may still find difficult to translate into business impact, he advocates for a narrative approach anchored in real-world events:

> *"One of the most effective ways to fill the gap is to **keep top management regularly informed about the evolving threat landscape.** Whenever a major data breach or cyber incident occurs, especially one affecting a company in a similar industry or with a comparable business model, it creates a valuable opportunity to brief management on lessons learned. Incidents such as the Marks & Spencer cyber incident in Q2 2025 can help make the risks more relatable."*

This is a deceptively simple but powerful insight. Abstract risk metrics struggle to compete for executive attention. A concrete incident at a recognizable peer organization does not. The CISO who brings the boardroom **a timely, well-contextualized briefing on a major industry incident** (explaining what happened, why it happened, what it cost, and what it would have taken to prevent it) is doing something fundamentally different from the CISO who presents a quarterly risk dashboard. They are making the invisible visible, and the theoretical tangible.

Marcus adds a structural dimension to this lesson. He argues that the relationship between cybersecurity and the business should be understood as a **partnership built on continuous dialogue**, not a one-way reporting mandate. This reframing matters: it shifts the CISO's role **from that of a technical expert seeking approval to that of a strategic partner** co-creating the organization's risk posture. And it carries a counterintuitive implication, that this dialogue may sometimes reveal that a new tool is not needed at all, and that **improving existing processes is the more effective and cost-efficient path forward**. In an environment where large organizations have been found to use more than 40 security tools on average, the discipline to resist unnecessary tool accumulation is itself a form of strategic value.

Philip, meanwhile, demonstrates what the destination looks like when this communication work has been done well over time. His organization has built **genuine Board-level consensus on cybersecurity, a foundation that transforms the annual budget conversation from a justification exercise into a strategic dialogue.** The lesson is that Board literacy is not a given, it is an achievement, built through sustained engagement, and the organizations that invest in it reap compounding returns.

The Lesson in Practice:

Make the invisible visible. *Use peer industry incidents as teaching moments. Translate technical risk into financial and operational impact. Build Board literacy as a long-term investment, not an annual presentation. And remember that the goal of the conversation is not approval, it is partnership.*

Lesson 2: AI is a Tool, Not a Strategy, Adopt it Accordingly

The survey finding that 86% of CISOs plan to increase AI/ML investment, against a backdrop of stable budgets, creates an apparent paradox. The practitioner interviews resolve it, but not in the way that AI enthusiasts might hope.

All three interviewees express interest in AI-powered cybersecurity tools. None of them treat AI as a strategic imperative in its own right. The distinction is important.

Adrian's organization takes a **cautious, evidence-first approach**: Proof of Concept and Proof of Value exercises are mandatory before any meaningful investment decision. The business case must be grounded in practical, measurable outcomes, reducing false positives, improving detection quality, keeping costs under control. AI is evaluated on the same terms as any other investment.

Marcus is the most direct in his caution:

"While there is growing stakeholder pressure to implement AI, ***the technology is not yet mature enough for broad cybersecurity application.*** *Security teams must remain rigorous in evaluating what they are actually paying for and whether the benefits justify the cost. Rapid AI adoption introduces new vulnerabilities, and the cyber skills gap has continuously increased. Ultimately,* ***adopting AI should never be treated as a business objective in itself****. The conversation is not approval, it is partnership."*

This is a bracing counterpoint to the sector's AI enthusiasm, and a necessary one. **The "AI-powered" label has become a marketing staple**, and Marcus's warning that it sometimes masks simple or superficial solutions is well-founded. The CISO who adopts an AI tool because it is AI, rather than because it solves a specific, well-defined problem, is not making a security investment; they are making a marketing decision.

Philip offers perhaps the most nuanced perspective. In his organization, AI adoption is neither mandated from the top nor resisted at the bottom, it **is emerging organically, driven by practitioners who are finding genuine use cases** in their day-to-day work:

"What we are seeing is a genuine bottom-up movement: people across the security function are exploring AI tools on their own initiative, finding practical ways to make their work faster, more efficient, and more effective. ***That organic adoption, grounded in real use cases, is far more sustainable than chasing a technology mandate.*** *When the value is demonstrable and the use case is concrete, the business case builds itself."*

This bottom-up, use-case-first model of AI adoption is the most sustainable path available to most organizations. It avoids the **twin failure modes of AI adoption:** the top-down mandate that generates investment without genuine use cases, and the blanket resistance that foregoes real efficiency gains out of excessive caution.

The Lesson in Practice:

Treat AI as a capability, not a category. *Before any AI investment, define the specific problem it will solve, the metric by which success will be measured, and the PoC/PoV process by which the claim will be validated. Create the conditions for bottom-up experimentation, and* ***let demonstrated value, not vendor marketing, drive the business case.***

Lesson 3: The GRC Crisis is Operational, Not Strategic, and the Fix is within Reach

The survey identifies compliance requirements as the number one driver of cybersecurity investment, while simultaneously revealing that most organizations still rely on in-house or fragmented GRC approaches. The practitioner interviews bring this paradox to life with striking operational specificity.

Philip's account of his organization's third-party risk assessment programme is the most vivid illustration in the entire research programme of what the GRC Paradox looks like in practice: **300+ vendors, managed through Excel spreadsheets**, assessed once a year, against a governance framework that requires four cycles annually. The gap between what the organization can deliver and what its own standards require is not a gap of intent, it is a gap of operational capacity, created and sustained by budget prioritization decisions.

Marcus confirms the broader trend. He notes that the regulatory landscape in Hong Kong and globally has become significantly more complex compared to a decade ago, with

regulatory fines increasing and businesses citing near-weekly regulatory shifts as their top compliance concern. He argues that **the shift toward third-party GRC solutions is not merely advisable, it is becoming inevitable:**

> *"Many organizations still rely on in-house or fragmented GRC approaches, which are increasingly unsustainable given the pace of regulatory change.* ***A shift toward third-party GRC solutions is therefore becoming inevitable.*** *As adoption grows across the industry, costs are expected to decrease, making these solutions progressively more accessible."*

Adrian adds the APAC-specific dimension: for organizations operating across multiple jurisdictions, data privacy laws and compliance requirements are changing frequently and in different directions simultaneously. His expectation is a **hybrid model, combining internal expertise with third-party GRC platforms**, that can manage different regulatory obligations across multiple jurisdictions, reduce duplicated assessment effort, improve workflow orchestration, and provide senior management with a clearer view of both compliance status and overall risk posture.

The **convergence of AI and GRC automation,** flagged by Philip, **represents the most significant near-term opportunity in this space.** The move from Excel-based GRC to AI-powered GRC platforms is not merely an efficiency improvement, it is a qualitative transformation in what the compliance function can deliver: continuous monitoring, automated risk scoring, real-time regulatory tracking, and management dashboards that make the compliance posture visible and actionable at the executive level.

The Lesson in Practice:

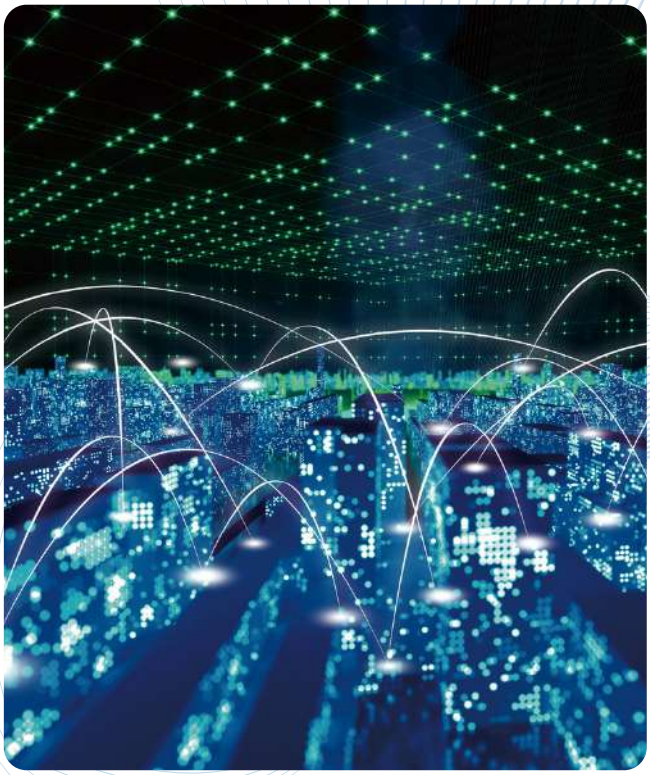
Stop treating GRC as a cost center and start treating it as a risk management capability. *If your compliance programme cannot meet the frequency requirements of your own governance framework, the problem is not the framework, it is the infrastructure.* ***Evaluate third-party GRC platforms now, with AI-powered automation as a key selection criterion.*** *The cost of inaction (in regulatory fines, audit findings, and reputational exposure) will exceed the cost of investment.*

Lesson 4: Vendor Selection Deserves a Framework: Here is One

The question of how to select cybersecurity vendors is one of the most practically consequential decisions a CISO makes, and one of the least systematically approached. The three interviewees offer a rich and complementary set of criteria that, taken together, constitute a robust vendor selection framework.

The most striking finding is the **divergence on vendor origin**. Philip explicitly de-prioritizes it (capability and cost are his primary criteria), and vendor headquarters are irrelevant provided the service quality is there. Adrian and Marcus take the opposite view, both flagging vendor origin and geopolitical risk as significant and growing considerations. Marcus provides the most detailed response:

> *For long-term investments spanning over five years, **the risk of a vendor being banned, sanctioned, or withdrawing from the market must be carefully assessed**, a risk that Gartner has also flagged as a key strategic consideration for security and risk management leaders. According to the World Economic Forum's Global Cybersecurity Outlook 2025, nearly 60% of organizations state that geopolitical tensions have directly affected their cybersecurity strategy."*[18]



This divergence is not a contradiction, it reflects the reality that different organizations, operating in different regulatory contexts and with different risk appetites, will weight these criteria differently. What matters is that the weighting is **explicit and deliberate**, not implicit and unconsidered.

Adrian's emphasis on **balancing risk, control, and sustainability** rather than choosing on price alone adds an important dimension: cost is a constraint, not a criterion. The question is not which vendor is cheapest, but which vendor delivers the best risk-adjusted value within the available budget.

Philip's emphasis on **responsiveness and quality of support** (the vendor's behavior when something goes wrong, not just when the contract is being signed) is perhaps the most underweighted criterion in formal procurement processes, and the one that most reliably predicts the quality of the long-term relationship.

[18] World Economic Forum, "Global Cybersecurity Outlook 2025", January 2025

Vendor Selection Checklist

The following checklist, derived directly from the practitioner interviews and validated against the survey findings, is offered as a practical tool for cybersecurity leaders approaching a vendor selection decision:

CAPABILITY & FIT

· Does the solution address a specific, documented gap in our current security posture?

· Has the vendor's capability been validated through a formal PoC or PoV exercise?

· Does the solution integrate effectively with our existing technology stack?

· Does it reduce false positives and improve detection quality in our specific environment?

· Is the solution aligned with our chosen security framework (e.g., NIST CSF, ISO 27001)?

COST & VALUE

· Does the total cost of ownership (licensing, implementation, training, ongoing support) fit within our budget envelope?

· Can we articulate a clear, measurable return on this investment — in risk reduction, efficiency gain, or compliance improvement?

· Are we choosing this solution because it delivers the best value, or because it is the cheapest option available?

· Have we assessed the cost of not investing — in regulatory exposure, operational risk, or capability gap?

VENDOR ORIGIN & GEOPOLITICAL RISK

· Where is the vendor headquartered, and where is our data processed and stored?

· Are there current or foreseeable geopolitical risks that could affect the vendor's ability to operate in our jurisdiction?

· For investments with a horizon of five years or more: what is the risk of this vendor being sanctioned, banned, or withdrawing from the market?

· Does the vendor's supply chain introduce third-party geopolitical exposure?

· Is the vendor's data sovereignty posture compatible with our regulatory obligations (e.g., PDPO, PCICSO, GDPR)?

SUPPORT QUALITY & RESPONSIVENESS

- What are the vendor's contractual SLAs for incident response and support?
- Have we spoken to existing customers about the vendor's responsiveness during actual security incidents?
- Is the vendor's support team locally accessible, or is support routed through a distant time zone?
- Does the vendor have a dedicated account team that understands our environment?

LONG-TERM PARTNERSHIP POTENTIAL

- Does the vendor behave like an extension of our team, or like a product company?
- Is the vendor transparent about product limitations, roadmap, and known issues?
- Does the vendor share context-aware threat intelligence relevant to our industry and region?
- Does the vendor invest in our team's capability — through training, knowledge sharing, and proactive enablement?
- Is the vendor present during incidents and challenges, or only at renewal time?

STRATEGIC & ARCHITECTURAL FIT

- Does this solution fit within a best-of-breed or platform strategy — and is that strategy deliberate?
- Have we assessed the vendor lock-in risk, particularly for platform investments?
- If this is a platform investment: what is the risk if the vendor changes its pricing model or product direction (cf. VMware/Broadcom)?
- Does this investment align with our three-to-five-year technology roadmap?
- Has this selection been reviewed with the CIO and CTO to ensure architectural alignment?

Lesson 5: The Technology Roadmap Must Be Living, Collaborative, and Risk-Anchored

The three interviewees describe technology roadmap processes that are meaningfully different from each other, and the differences are instructive.

- Philip's approach is **audit-anchored and rolling**: a three-year roadmap, reviewed annually, driven by audit findings that translate identified gaps into specific technology requirements. The CIO and CTO are part of the review process, ensuring that security technology decisions are made in the context of the broader IT architecture. The DNS tunnelling example, a specific audit finding translated directly into a specific tool requirement, illustrates the discipline of this approach: investment decisions are grounded in evidence, not aspiration.

- Adrian's approach is **risk-based and zero-trust-aligned**, with a deliberate stance on the best-of-breed versus platform debate. His position, a hybrid model that groups several functions into one platform while keeping sensitive or specialized areas in separate products, reflects a sophisticated understanding of the trade-offs involved. The VMware/Broadcom example is a timely reminder that platform consolidation carries its own risks: pricing model changes, product discontinuation, and the concentration of vulnerability across multiple defense layers in a single product.

- Marcus raises the most urgent structural concern: the strategic partnership between CIOs and CISOs is often lacking, and when these two functions operate in silos, organizations face missed opportunities, increased risks, and operational inefficiencies. His recommendation, that IT roadmaps be reviewed on an annual basis rather than the traditional three-to-five-year cycle, and that security strategy be connected to business strategy through regular scenario planning and risk assessments, the pace at which the technology and threat landscape is now evolving. This is consistent with Gartner CISO Communities' priorities for 2026, which identify the alignment of security strategy with business strategy as a critical imperative.

The Lesson in Practice:

Your technology roadmap is only as good as the process that produces it. *It must be anchored in evidence (audit findings, risk assessments), collaborative (CIO, CTO, and business leadership must be part of the conversation), and living (reviewed at least annually, not on a three-to-five-year cycle). And it must take an explicit position on the platform versus best-of-breed debate, because the absence of a position is itself a decision, and usually not a good one.*

Lesson 6: The Structural Problem is Silos, and Everyone Knows it

The closing question *(What would you change, and what is stopping you?)* produced the most candid and convergent responses of the entire interview programme.

Adrian's answer focuses on the **investment decision process**: he would make decisions more consistently based on capability fit, measurable security outcomes, and long-term value, rather than short-term cost considerations. What stops him is the pressure to optimize for immediate budget constraints, a structural tension that no individual CISO can resolve alone.

Philip's answer is **budget**: with more resources, there would be more freedom to select best-in-class tools without compromise. The tension between security ambition and budget reality does not go away; you learn to manage it as effectively as possible.

Marcus's answer is the most structurally ambitious, and the most honest about why it remains unrealized:

> *"**IT and Security teams must define common objectives together.** The core problem is that organizations tend to work vertically, each department operating with its own agenda, policies, and priorities, rather than collaborating horizontally across functions. While there is broad rational agreement on the need for cross-functional alignment, internal politics and competing departmental interests continue to prevent it from being realized in practice."*

This is a finding that resonates far beyond cybersecurity. The **silo problem** is one of the most persistent and well-documented challenges in organizational management, and the fact that everyone agrees it needs to be solved, while it continues not to be solved, tells us something important: **the barrier is not knowledge, but incentive**. Departments are structured, measured, and rewarded in ways that reinforce vertical operation. Changing that requires not just rational agreement but structural intervention, changes to governance, measurement, and incentive design that make horizontal collaboration the path of least resistance rather than the path of most resistance.

The Lesson in Practice:

*Acknowledge the silo problem explicitly, and address it structurally. Rational agreement is not enough. **If you want CISOs and CIOs to collaborate on technology roadmaps, build that collaboration into the governance process**, make it a standing agenda item, a shared accountability, a joint deliverable. The organizations that will navigate the next decade of cybersecurity complexity most effectively will be those that have broken down the walls between security, IT, and business, not because everyone agreed it was a good idea, but because the structure made it inevitable.*

Looking Forward: Five Imperatives for the Cybersecurity Leader of 2026 and Beyond

Drawing together the survey findings, the practitioner interviews, and the broader research programme, five imperatives emerge for cybersecurity leaders navigating the years ahead:

1. Invest in Board literacy as a strategic asset. The organizations that have built genuine Board-level cybersecurity understanding (as illustrated by Philip's experience) operate in a fundamentally different and more effective governance environment. This is not achieved through annual presentations; it is achieved through sustained, contextualized, narrative-driven engagement that makes cyber risk real and relatable to non-technical leaders.

2. Build the measurement infrastructure before you need it. The inability to measure the return on cybersecurity investment is not just a reporting problem. it is a governance failure that undermines every investment decision. Organizations that invest now in building formal ROSI measurement frameworks will be better positioned to justify investment, demonstrate value, and make evidence-based allocation decisions in an environment of stable or constrained budgets.

3. Treat GRC automation as a strategic priority, not an operational nicety. The regulatory environment is not going to become simpler. The organizations that invest now in third-party GRC platforms, particularly those with AI-powered automation capabilities, will build a compliance infrastructure that scales with regulatory complexity. Those that continue to rely on Excel and in-house tools will find themselves increasingly unable to meet their own governance standards, let alone the expectations of regulators and auditors.

4. Adopt AI with discipline, not enthusiasm. The AI investment wave is real, and the efficiency gains available to cybersecurity functions are genuine. But the path to sustainable AI adoption runs through rigorous use-case definition, formal PoC/PoV validation, and bottom-up practitioner experimentation, not top-down mandate or vendor marketing. The CISO who can say precisely what problem their AI investment solves, and precisely how they will know if it has solved it, is the CISO who will get lasting value from that investment.

5. Break the silos structurally, not rhetorically. The alignment of cybersecurity with IT strategy, business strategy, and Board governance is the defining organizational challenge of the next decade. It will not be achieved through goodwill alone. It requires structural intervention: joint governance processes, shared accountability frameworks, and incentive designs that reward horizontal collaboration. The organizations

Closing Reflection

The three practitioners whose voices animate this final chapter are, in many respects, different leaders operating in different contexts with different constraints. But they share something important: a clear-eyed, pragmatic, and deeply experienced understanding of what cybersecurity leadership actually requires in practice.

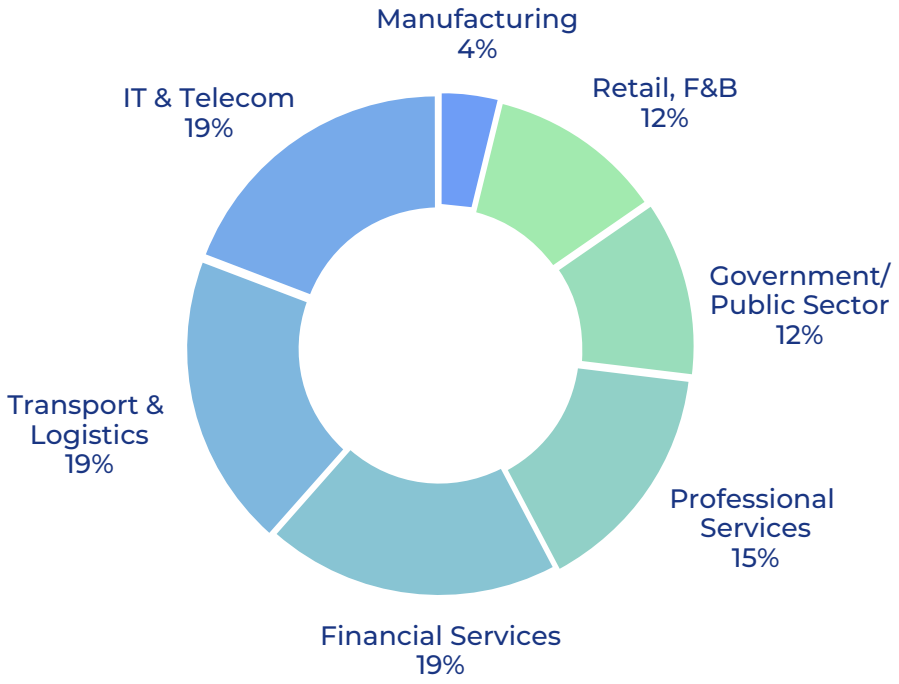
What emerges from their collective wisdom is not a set of silver bullets, but **a set of disciplines:** the discipline of evidence-based investment justification; the discipline of rigorous vendor evaluation; the discipline of collaborative roadmap planning; the discipline of treating AI as a capability rather than a category; and the discipline of building the governance infrastructure that makes all of the above possible.

These disciplines are not glamorous. They do not generate headlines or conference keynotes. But they are, in the end, what separates the cybersecurity functions that consistently deliver value from those that consistently struggle to justify their existence.

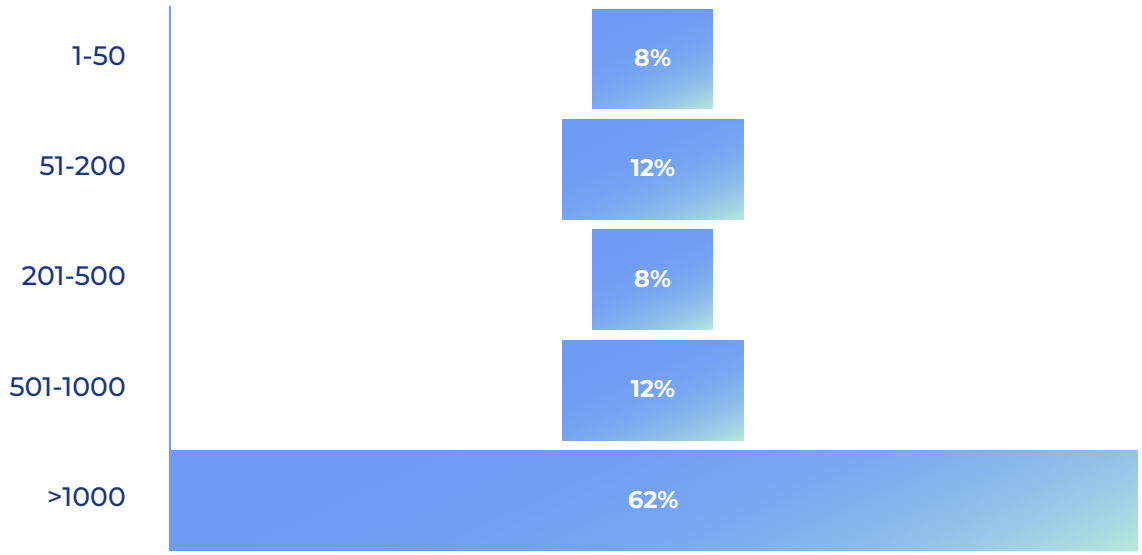
The data tells us where the sector is. The practitioners tell us how to move it forward. The choice of whether to act on that wisdom belongs to the reader.

Appendix

Survey Participants by Industry



Survey Participants by Organization Size in Hong Kong



中國香港網絡安全協會
HONG KONG CHINA NETWORK SECURITY ASSOCIATION

SIA

Key Contacts

Jolly Liang
Marketing & PR Manager
HKCNSA
jolly.liang@hkcnsa.org

Stefano Fois
Research Director
HKCNSA
stefano.fois@hkcnsa.org

Michael Pang
Head of Cybersecurity APAC
Sia
michael.pang@sia-partners.com