

Towards a Cybersecure APEC

BUILDING A
SHARED
REGIONAL
PLATFORM FOR
CYBERSECURITY

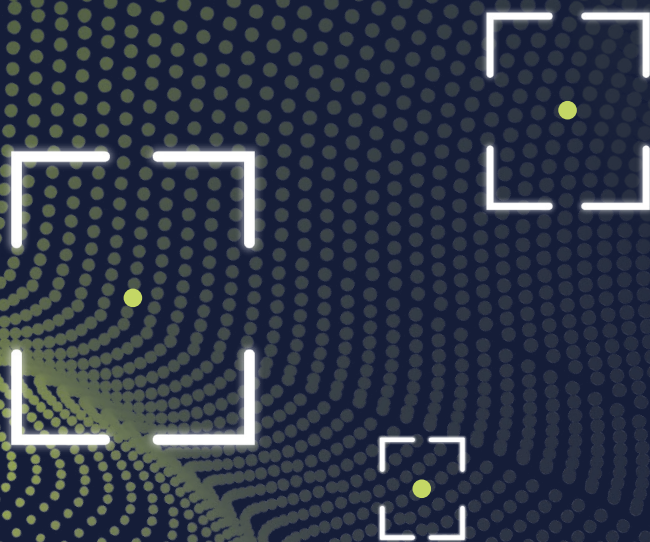


TABLE OF CONTENTS

Foreword	3
Introduction	4
A regional platform for cybersecurity	7
Leveling up: cybersecurity capacity building	8
A networked approach for talent development	10
An enabling regulatory environment (coordination and alignment)	14
Information sharing in the age of hyper-attacks	15
MSME Support	17
Conclusion: the time for action is now	18
Acknowledgments	19
ABAC Cybersecurity Symposium Speakers	20
Endnotes	21

FOREWORD

Nearly two-thirds of the global economy is already digitalized.¹ Accelerated by the COVID-19 pandemic, digital transformation continues to revolutionize how we do business, interact with one another, and solve our most intractable problems. The advent of ubiquitous connectivity combined with exponential growth in data will only continue to propel us towards a digital-first era characteristic of an advanced digital economy.

However, as we build towards this vision of a prosperous and inclusive digital economy, the lack of a strong cybersecurity framework for the APEC region imperils the promise of digitalization and casts a shadow on our brightest forecasts for the economy.

APEC finds itself at an urgent moment. The confluence of emergent technologies; increasing digital skills; and continued development of physical, data, and foundational digital infrastructure presents the ideal opportunity for establishing a coherent, strategic, and durable cybersecurity framework. Inaction at this critical juncture would jeopardize economic and social gains enabled by digitalization and potentially compromise critical infrastructure across APEC.

As the top concern for businesses, consumers, and society at large, cybersecurity is foundational to a thriving and inclusive digital economy. It is the challenge of our time, and it cannot be solved unilaterally. Yet, developed strategically, a collaborative and resilient cybersecurity posture is an opportunity that can generate an economic ripple effect that would embolden businesses and consumers, attract investment, boost productivity, and increase regional trade.

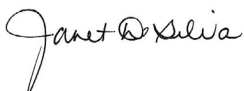
Recognizing its foundational nature and enabling effect, as well as the necessity for a collaborative approach to

achieve success, the APEC Business Advisory Council (ABAC) sought to examine the state of cybersecurity in APEC. At a symposium held in April 2022, ABAC convened experts from business, academia, and government agencies to discuss how we can best strengthen cybersecurity across APEC. Their insights and inputs along with research conducted by ABAC informed the findings of this report.

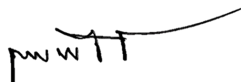
The key contributions of this report are neither technical nor prescriptive on what must be done to achieve cybersecurity. Indeed, APEC and its member economies have, to varying degrees, acknowledged the importance of cybersecurity and recognized the significance of action in this critical sector.

Rather, this report recognizes that a collective challenge requires a collective response. In this context, it presents a strategy on how best to achieve the common goal of a strengthened cybersecurity posture. It puts forward a multilateral framework through a regional platform for cybersecurity that would provide a mechanism for cooperation on cybersecurity. The regional platform would mobilize resources, provide key data, and monitor progress towards cyber resilience. It would catalyze action strategically by addressing the toughest cybersecurity challenges including capacity building, talent development, regulatory alignment, information sharing, and support for micro, small and medium-sized business (MSMEs).

To protect the promise of digitalization, we must integrate cybersecurity into the fibre of the digital economy and make it a topic at the board table, the cabinet office, in our schools and within our MSMEs. This report contributes to this effort by outlining how APEC economies, businesses, and academia can cooperate to strengthen regional cybersecurity.



Jan De Silva
Chair Digital Working Group



Kriengkrai Thiennukul
ABAC Chair

INTRODUCTION

The same features that enable our economies to thrive – technology adoption, growth in e-commerce revenue, the internet of things connectivity, and a high degree of mobile internet traffic also intensify our cyber risk.

The COVID-19 pandemic remains a watershed moment for digitalization. It accelerated the adoption of digital technologies across the economy and expanded digital maturity.² This has allowed many businesses to weather the economic crises and closures wrought by COVID-19, and in some cases, increased efficiency, and access to new markets. While this has been an economic boon, it has increased vulnerability and resulted in weakened cyber defenses for businesses, consumers, and related supply chains. In the rush to innovate and respond to increased demand, 81% of organizations sidestepped cyber processes neglecting to consult cybersecurity teams when planning new business initiatives.³

Indeed, the same features that enable our economies to thrive – technology adoption, growth in e-commerce revenue, the internet of things connectivity, and a high degree of mobile internet traffic also intensify our cyber risk. While this is a global trend, the Asia Pacific Risk Centre, has declared the region “a perfect cyber storm” due to its increased likelihood of attack - 80% more than the rest of the world.⁴

APEC recognized critical operational and digital infrastructure were at serious risk in 2001 when it made clear the importance of “strengthening of activities in the area of critical sector protection, including telecommunications, transportation, health, and energy.”⁵ Since then, cyber risks and attacks have only increased in volume and sophistication with the evolution of the digital economy increasingly putting consumers, businesses, and underlying operational and digital infrastructure at risk. Yet, as attacks and attackers advanced and proliferated in the proceeding years, APEC’s capabilities to effectively respond and deter them have not kept pace.

81%

of organizations sidestepped cyber processes neglecting to consult cybersecurity teams when planning new business initiatives.

By 2025, the cost of cyber-attacks is estimated to be:

Globally

USD 10.5 trillion

Asia Pacific Region

USD 1.75 trillion

INTRODUCTION

This status quo perpetuates significant economic costs that could potentially slow growth. This is unsurprising as 70% of attacks are financially motivated.⁶ Through ever-expanding modes of attack and the subsequent sale of sensitive data on the deep web, the opportunities for financial returns on trade in stolen data and intellectual property proliferate. By 2025, the cost of cyber-attacks is estimated to be USD 10.5 trillion globally and USD 1.75 trillion in the Asia Pacific region.^{7,8} In other words, cybercrime will be the single largest criminal segment worldwide – more profitable than the trade in illicit drugs.

Conversely, cybersecurity is an investment that secures the long-term benefits of digitalization and represents an opportunity for the region. The global information security sector is projected to be worth USD 376 billion by 2029.⁹ Cultivated strategically, responses to the cybersecurity challenge in APEC can be the secret to seizing global growth and leadership opportunity for the region. Whether it is developing world-class talent, innovative security tech, or leading global approaches and standards setting, there are multiple pathways to seizing this opportunity.



70% of attacks are financially motivated

INTRODUCTION



As the region competes for a place amongst the world's leading digital economies, it will face increased vectors for cyber-attacks. The absence of a comprehensive framework for cybersecurity – including limited strategies, policies, cooperation, and requisite oversight - has resulted in a lack of cyber resilience and readiness across APEC. APEC's cybersecurity industry faces shortages in its capabilities and expertise, varied operating models, an underestimated value-at-risk, and fragmented programs which will lead to operational complexity and will continue to pose a significant risk.

It is increasingly evident that cybersecurity is a precondition for a thriving and inclusive digital economy across the region. APEC economies must therefore implement and coordinate cybersecurity strategies to protect consumers and businesses and avoid the potential costs and negative effects on regional trade and investment.^{10,11}

The approach to cyber must be aligned and integrated to build the infrastructure and talent necessary to safeguard economic growth and innovation. To achieve this, APEC should establish a regional platform for cybersecurity to protect businesses, consumers, and our underlying digital and operational infrastructure. This cooperative approach would improve the cybersecurity ecosystem and respond to the needs of the business community for leadership.¹²

A REGIONAL PLATFORM FOR CYBERSECURITY



An APEC regional platform for cybersecurity would coordinate action and investment and would address APEC declarations on cybersecurity supporting the implementation of updated strategies and action plans. The platform would serve as a voluntary regional vehicle and forum for coordinated action. It would be aligned towards the common objective of moving APEC towards cyber resiliency. In doing so, it would:

- Identify, replicate, and scale best practices in cybersecurity across the region; this would include best integrating best practices found outside the region through partnerships
- Mobilize funding and resource to emerging and developing economies to increase capacity; and
- Facilitate public, private, and academic partnerships on cybersecurity.

The regional platform would also require new ways of thinking around what effective cross-sectoral collaboration could look like. APEC must determine how best to enable, incentivize, and invest in the private sector and academic collaborations to counteract the financial incentives of cybercrime.

To enable this, ABAC recommends the platform conduct periodic studies of cybersecurity capabilities in the region to clarify current baseline starting points, gaps and required best practices.

CONDITIONS FOR SUCCESS



Capacity building across APEC



Regulatory coordination and alignment



MSME supports



Talent development



Information sharing

A REGIONAL PLATFORM FOR CYBERSECURITY



LEVELING UP: CYBERSECURITY CAPACITY BUILDING

Cybersecurity preparedness is vital to the proliferation of Information and Communications Technologies (ICT) and closing the digital divide. While foundational, however, the digital divide is not the only gap that will need to be addressed. Although APEC does not currently measure cybersecurity capacity amongst its member economies, global cybersecurity indexes, show clear and significant gaps that must be closed between APEC economies.^{13,14}

The Global Cyber Security Capacity Centre (GCSCC) defines cybersecurity capacity as comprising of five dimensions that an economy requires to effectively deliver cybersecurity.¹⁵ These include:

- Developing cybersecurity policy and strategy
- Encouraging responsible cybersecurity culture within society
- Building cybersecurity knowledge and capabilities
- Creating effective legal and regulatory frameworks
- Controlling risks through standards and technologies.



A REGIONAL PLATFORM FOR CYBERSECURITY



The GCSCC's accompanying capacity maturity model (CMM)¹⁶ assess the ability of each economy against the five dimensions above categorizing them in the stages of start-up; formative; established; strategic; and dynamic.

To design effective, regional capacity building programs, it is important to understand existing gaps and opportunities across the region. APEC should conduct an annual or biannual regional cybersecurity capacity study. The results of these studies should inform targeted capacity building projects and programs using the GCSCC and CMM as models to raise the collective capacity of the region to prevent and respond to cyber-attacks.



ABAC RECOMMENDS THAT APEC:

Establish a platform for cybersecurity that would support capacity building efforts by:

- Conducting an annual or biannual review of the region's cybersecurity capacity utilizing the GCSCC's CMM as a model;
- Establishing a regional cybersecurity capacity baseline and support attainment and alignment with international standards; and
- Establishing a regional forum for cybersecurity capacity building that would support regional attainment of international cybersecurity capacity standards.

A REGIONAL PLATFORM FOR CYBERSECURITY

A NETWORKED APPROACH FOR TALENT DEVELOPMENT

Digitization has meant that demand for digitally skilled workers has far surpassed the available supply.¹⁷ The cybersecurity sector is no different. Recent studies report talent shortages as a major challenge to responding to a cyberattack.^{18,19} The APEC Region has an estimated shortage of more than 1.8 million cybersecurity jobs, the world's highest.²⁰ In addition, the 2021 Ernst Young Global Information Security Survey found that 73% of Asia Pacific businesses experienced an increase in disruptive cyber incidents.²¹ Taken together with the capacity challenges discussed above and an increased attack surface due to the exponential growth of connected devices, this persistent talent gap puts the region at an elevated risk and hinders its capacity to respond to the growing number of incidents.

The magnitude of the challenge requires a networked approach to ensure targeted short, medium, and long-term solutions. A networked approach is one that unites relevant stakeholders to address the talent shortage strategically. In addition to appropriate investments and a clear strategy, the collaboration between government, business, academia, and civil society will be an essential element of the networked approach.

BUILDING A CULTURE OF CYBERSECURITY

Good people make bad security choices. According to the World Economic Forum's (WEF) 2022 Global Risks Report, 95% of cybersecurity issues can be traced to human error.²² The role of the individual in mitigating cyber incidences cannot be overstated. Cybersecurity awareness and continuous employee training are therefore vital components of any strategy to build and improve cybersecurity maturity and resilience. APEC must develop and fortify its own "human firewall" to extend its capability. Governments must thus mainstream the development of cybersecurity awareness and skills amongst the general population as a first step. This has the dual effect of ensuring that individuals are aware of the risks and highlights a potential cyber career path.



The APEC Region cybersecurity jobs has an estimated shortage of more than

1.8m

73%

of Asia Pacific businesses experienced an increase in disruptive cyber incidents.

95%

of cybersecurity issues can be traced to human error.

A REGIONAL PLATFORM FOR CYBERSECURITY



SHORT TERM: MICRO-CREDENTIALING AS A BRIDGE AND A PATHWAY TO REDUCE THE TALENT GAP

Contrary to popular belief, cybersecurity is not strictly a technical career field, it requires a diverse set of skills. With such a deep talent shortage, micro-credentialing programs offer a bridge to address both immediate needs and create a pathway into a sustainable career in cybersecurity. These programs are critical for long-term resiliency in the region. Both businesses and academia are increasingly partnering to provide micro credentialing programs. While initiatives exist in the APEC region, they are not nearly enough to develop necessary talent. Programs must be long-term and institutionalized to continue feeding the talent pipeline. They must also be available across the region rather than in pockets as is currently the case.



What could this look like?

- Rogers Cybersecure Catalyst at Toronto Metropolitan University is Canada's leading centre for training, innovation, and collaboration in cybersecurity. Its Accelerated Cybersecurity Training Program (ACTP) is an innovative approach to rapid workforce development in Canadian cybersecurity, leveraging public, private, and academic partnerships to meet the labour needs of employers and make the sector more accessible to people from diverse backgrounds. Other initiatives, like CyberStart Canada, help to spark interest in cybersecurity in high school-aged youth.
- Salesforce, a leading global technology brand in partnership with the World Economic Forum and the Global Cyber Alliance has established the Trailhead Program, to introduce and shepherd new recruits on their cybersecurity journey/careers.
- Workshops to Empower Women in Cyber Risk Management Malaysia are embracing the challenge of increasing diversity within the cybersecurity industry and empowering women. This is part of a broader program to develop "industry ready" cybersecurity practitioners that includes a **Cyber First Program for youth 12 – 17**.
- In New Zealand, Microsoft has partnered with TupuToa a social enterprise focused on growing Māori and Pacific leaders to equip youth with the knowledge and skills needed to become security professionals. This part of Microsoft's efforts to develop cybersecurity skills across 23 countries.

MEDIUM AND LONG TERM: DEVELOP SPECIALIZED SKILLS

Cybersecurity is a generational challenge that requires sustainable solutions. The current talent gap will continue to grow as the region continues to digitally transform. The digital and economic growth potential in developing and emerging economies is enormous as nearly 40% of the population is yet to be connected.²³ We must therefore extend the pipeline by updating school curricula to develop the basic skills and interest needed to inspire rewarding careers in cybersecurity. Economies implementing such strategies are already reaping the benefits not only in reducing the talent shortage but in attracting cybersecurity businesses and investment.

In addition, building skills and partnerships should not mean privileging university or college education, sidelining those that might have an interest and complementary skills, but lack post-secondary degrees. Instead, a holistic approach to cybersecurity talent that considers a wide range of experiences including hands-on experience, professional certifications, and post-secondary education should be undertaken. Governments can also have an important role in scaling programs that work across their economies to allow more people to participate. This would require increased funding and communication about such programs.

The digital and economic growth potential in developing and emerging economies is enormous as nearly 40% of the population is yet to be connected. We must therefore extend the pipeline by updating school curricula to develop the basic skills and interest needed to inspire rewarding careers in cybersecurity.

A REGIONAL PLATFORM FOR CYBERSECURITY



What could this look like?

- The province of New Brunswick in Canada decided to make cybersecurity a priority and took an ecosystem approach working closely with academia and the private sector. As part of this endeavour, the education system was also updated with a new curriculum to deliver the basic skills necessary for cybersecurity in younger age groups (elementary and high school). In addition, challenges and hackathons raised awareness of cybersecurity as a viable, rewarding, career amongst young people – particularly those who were marginalized – across the province. This resulted in the creation of hundreds of cybersecurity jobs. IBM, Siemens, and other cybersecurity businesses established global centres of excellence for cybersecurity in New Brunswick as a result. This ecosystem approach is essential to building cyber resiliency.
- Vietnam has announced that it will include cybersecurity education in its high school curriculum to increase the basic skills necessary to build a cyber talent pool and introduce cybersecurity a rewarding career.

The reality is that to remain on par with market growth of the cybersecurity/information security sector, the current capacity must be more than doubled. To become a leader, APEC must further capacity and invest in the growth of research and innovation within the field.



ABAC RECOMMENDS THAT APEC:

Establish a platform for cybersecurity that would support talent development in APEC by:

- Developing regional talent development programs in partnership with the public and private sector, government, and academia;
- Replicate and scale successful programs across the region; and
- Share best practices on public cyber hygiene through campaigns.

AN ENABLING REGULATORY ENVIRONMENT (COORDINATION AND ALIGNMENT)

In 2002, APEC Ministers and Leaders committed to promote cybersecurity by “enacting a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with the provisions of international legal instruments, including United Nations General Assembly Resolution 55/63 (2000) and Convention on Cybercrime (2001), by October 2003.” Nearly 20 years later, APEC does not have a harmonized or coordinated legal approach to cybersecurity or cybercrime. The gaps and inconsistencies in APEC legislations, standards, and guidelines provide a haven for bad actors to exploit. They also pose an administration and compliance challenge for businesses that would increase costs for operating in the region.

Currently, only eight APEC economies are signatory to the Budapest Convention on Cybercrime, an international treaty that seeks to address cybercrime by harmonizing laws, improving legislative techniques, and increasing cooperation. APEC signatories include Australia, Canada, Chile, Japan, New Zealand, Peru, Philippines, and the United States.²⁴

While the Budapest Convention offers a pathway to coordination and harmonization of APEC’s cybersecurity regulatory environment, it is not the only one. APEC should establish a process to achieve coordination and alignment of cybersecurity regulations that considers the evolution of the digital economy. This should include best practices and a process-based approach to enhancing cybersecurity as established in the APEC Framework to Secure the Digital Economy and APEC Cybersecurity Strategy. Achieving this will help to address cybercrime, standardize cyber incident reporting requirements, and reduce compliance and administration costs for businesses operating in the region.

As cybercrime accelerates to become the world’s largest criminal segment, APEC must shore up defences and investments to prevent attacks – it must declare a war on cybercrime. APEC’s capacity must evolve from a defensive posture to one that enables effective countermeasures across the region.

The gaps and inconsistencies in APEC legislations, standards, and guidelines provide a haven for bad actors to exploit.



ABAC RECOMMENDS THAT APEC:

Establish a platform for cybersecurity that would support regulatory alignment in APEC by:

- Providing an annual update on progress towards regulatory alignment and adoption of international standards and best practices;
- Support businesses in understanding compliance requirements across the region; and
- Create a one-stop-shop for regulatory standards and compliance requirements.



INFORMATION SHARING IN THE AGE OF HYPER-ATTACKS

The 2002 APEC Cybersecurity Strategy identified information sharing as one of the areas that would “serve as the basis of APEC’s efforts on cybercrime and critical infrastructure protection.”²⁵ The 2019 APEC Framework for Securing the Digital Economy also highlighted the importance of information sharing and encouraged APEC member economies to:

- Promote information sharing around current risks and risk management practices among stakeholders and member economies through economy-level Computer Security Incident Response Teams (CSIRTs) and other networks.
- Foster information sharing among stakeholders.

One recommendation to implement the 2002 APEC Cybersecurity Strategy was for APEC member economies to join multilateral frameworks for information sharing such as the G7 24/7 Cybercrime Network. To date, only seven economies have joined this network. No APEC specific network that brings together public and private actors for information sharing currently exists.

Furthermore, the APEC Security and Prosperity Steering Group released the APEC Cooperative Response in Cross-Border Environment Guidelines²⁶ in 2008 to assist APEC economies to strengthen cooperative incident response capabilities. While APEC continues to discuss the communication of cybersecurity practices²⁷ and approaches, more needs to be done to share critical information to help protect the region.

A REGIONAL PLATFORM FOR CYBERSECURITY

90% of survey respondents reported receiving actionable insights from external information-sharing groups and/or partners.²⁸ Yet, globally the number of businesses sharing information openly is only 35%.²⁹

Private sector information sharing networks such as the [Global Resilience Federation](#) do exist. However, to provide better protection, a partnership between public and private sectors on regional information sharing is critical, especially for MSMEs that may not have resources and/or expertise to be part of large membership based private sector groups. The 2022 WEF Global Cybersecurity Outlook found over 90% of survey respondents reported receiving actionable insights from external information-sharing groups and/or partners.²⁸ Yet, globally the number of businesses sharing information openly is only 35%.²⁹ Business executives cited the lack of protections such as anonymity and information usage agreements; process issues such as a lack of information disclosure agreements; the need for legal protections against civil or criminal lawsuits; and direct access to law enforcement as barriers to increased information sharing.³⁰

As more and more jurisdictions initiate incident reporting requirements, business compliance and administrative costs in the region will continue to increase.³¹ A shared platform could potentially make this process more efficient with a single point of reporting for all businesses operating across APEC.



ABAC recommends that APEC:

Establish a platform for cybersecurity that would support information sharing in APEC by:

- Developing and building ISACs across the region in partnership with the private sector and supporting the coordination of threat intelligence and information sharing relevant to APEC members; and
- Instituting a one-stop-shop for information sharing for APEC that would allow for ease of compliance and administration;
- Supporting the easing of regulatory restrictions on information sharing.



What could this look like?

- The [Microsoft Asia Pacific Public Sector Cyber Security Executive Council](#) seeks to provide a forum for exchange of information on cyber threats and cybersecurity solutions. The council which is a public and private partnership aims to build a community where threat intelligence, technology, and resources can be shared in a timely and open manner. It includes 15 policy makers from Brunei, Indonesia, Republic of Korea, Malaysia, Philippines, Singapore, and Thailand, supported by cybersecurity professionals from Microsoft.
- **Information Sharing and Analysis Centres (ISACs)** are non-profit organizations that provide a central resource for gathering information on cyber threats (in many cases to critical infrastructure) as well as allow two-way sharing of information between the private and the public sector. ISACs have created communities within the private sector. They could be oriented on a specific critical sector (e.g., finance, energy, health) or serve as a focal point on the national level to gather information about cyber incidents and analyse it.

A REGIONAL PLATFORM FOR CYBERSECURITY

MSME SUPPORT

MSMEs make up 97% of businesses and employ half the workforce in APEC.³² The OECD estimates that 70% of MSMEs worldwide have intensified their use of digital technologies due to COVID-19.³³ The digital transformation of MSMEs has increased their exposure to cybersecurity risks. Because of this, they are the targets of cyberattacks 43% of the time.³⁴ Given that they are less likely to have the financial and human resources to respond well and protect themselves, more than 60% of MSMEs go out of business within six months of a cyberattack.³⁵ This is partly because nearly 80% of attacks of very small businesses are ransomware attacks according to Verizon's 2022 Global Data Breach Incident Report³⁶ thanks in large part due to the proliferation of ransomware as a service. There are also significant information gaps when it comes to cybersecurity education and culture within MSMEs.

According to a report by CISCO, 56% of SMEs in the Asia Pacific have experienced a cyber-attack in the last 12 months.³⁷ The same report found that three-quarters of SMEs fear that a cyber-attack could end their entire business.

Considering the economic contribution of MSMEs in the APEC region – between 40% to 60% of GDP in most economies³⁸ – MSME vulnerabilities pose a serious security and economic risk for the region. MSMEs are also integrated into supply chains – their vulnerability can have systemic and supply chain shocks for the region.

One of the key recommendations of the ABAC Digital First Economy Whitepaper³⁹ is to promote cloud adoption, including cloud-first policies and support for cloud migration. This would not only accelerate vertical industry digitalization, but it has the added impact of strengthening MSMEs capabilities by reducing costs, enabling scale, and lowering barriers to innovation.⁴⁰ Security and privacy are cited as one of the most important factors for cloud adoption globally⁴¹ because it is one of the quickest ways to safeguard MSMEs. APEC economies should encourage and provide support for cloud migration to enhance the cyber-resilience of MSMEs.

More than

60%

of MSMEs go out of business within six months of a cyberattack.



What could this look like?

The [Australian Indonesian Centre's Skills Futures Program](#) offers cybersecurity courses to MSMEs to build their cyber resilience. It provides small business owners a series of webinars and offline exercises on cybersecurity and global trade and aims to reduce the range of cyber threats and risks to growing a business. In addition, it supports MSMEs to understand the regulations of digital trade including the protection of personal data as well understanding the commercial opportunities that are becoming available to them.



ABAC RECOMMENDS THAT APEC:

Establish a platform for cybersecurity that would support MSMEs in APEC to meet the cybersecurity challenge by:

- Supporting MSMEs to increase the adoption of more sophisticated security practices and tool in partnership with private sector; and
- Partner with large firms across the region to provide resources and information on building a culture of cybersecurity.



CONCLUSION: THE TIME FOR ACTION IS NOW

APEC recognized the importance of cybersecurity and collaboration within the region to protect the digital economy in 2002 through APEC Cybersecurity Strategy. In the intervening years, it has reinforced this recognition with frameworks for action across the region. Yet, it has been exactly the kind of coordinated regional action necessary to support implementation of the APEC Cybersecurity Strategy that has been missing for the last twenty years. The threat landscape has transformed incredibly since 2002, and while the principles of the APEC Strategy – namely collaboration – remain relevant today, principles alone will not be enough to protect the region from increasing cyber incidents. APEC needs a driver to support the implementation of its cybersecurity strategy. It should establish a shared regional platform that would provide the necessary research, coordination, and mechanism for collective action from public, private, and academic organizations across the region for the digital first era.



ACKNOWLEDGMENTS

This report would not have been possible without the generous support of Global Affairs Canada and the Government of Canada who funded the research as well as the table-setting Cybersecurity Symposium that occurred at the second meeting of the APEC Business Advisory Council (ABAC) in April 2022. We are grateful to the team who ensured the event was a success and allowed the ideas and insights of our speakers to shine. This symposium was a critical look at the state of cybersecurity in APEC and was informative in developing the recommendations found herein.

The contributions and reviews of the speakers at the symposium – leaders within their businesses and the cybersecurity sector – were essential in guiding the research questions and focusing our efforts on best practices and innovations that could help revitalize cybersecurity in APEC. They are listed below.

Finally, the support of the Asia Pacific Foundation of Canada and the Toronto Region Board of Trade was critical to executing the Cybersecurity Symposium and finalizing the research for this paper. Thank you to Roselle Martino, Reid McKay, Stephanie Lee, Jeff Lang-Weir, and Megan Stangl.

We would also like to acknowledge the support of the ABAC Digital Working Group (DWG) Co-Chairs and their teams in shaping the DWG agenda for 2022 and for their reviews, comments, and suggestions on this paper, as well as their continuing support in helping to shape a vision for a thriving and inclusive digital economy in APEC.



Global Affairs
Canada
Affaires mondiales
Canada



ASIA PACIFIC FOUNDATION OF CANADA FONDATION ASIE PACIFIQUE DU CANADA



ACKNOWLEDGMENTS

We are also grateful to the following industry experts for their comments and reviews which have strengthened the recommendations found herein.

John McClurg
Sr. Vice President and Chief Information Security Officer, Blackberry

Richard Wunderlich
Cyber Research and University Relations, Siemens Canada Limited

Charmaine Valmonte
Chief Information Security Officer, Aboitiz Group



This report was written by Ige Egal, Policy Director for Digital Innovation at the Toronto Region Board of Trade and Lead Staffer at the APEC Business Advisory Council (ABAC) Digital Working Group. Design was provided by Lisa Davison Design.

ABAC CYBERSECURITY SYMPOSIUM SPEAKERS

Dr. Chaichana Mitrpant
Executive Director, Electronic Transactions Development Agency (ETDA)



John Chen
Executive Chairman & Chief Executive Officer, BlackBerry Limited



Charles Finlay
Founding Executive Director, Rogers Cybersecure Catalyst, Toronto Metropolitan University



John Weigelt
National Technology Officer, Microsoft Canada



David Shipley
Co-founder and CEO, Beauceron Security



Kobsak Duangdee
Secretary General, Thai Banker's Association (TBA)



Dhruva Suthar
Director of Security, IBM Canada



Michaela Browning
VP, Government and Public Policy, Google Asia Pacific



Faisal Kazi
President, and Chief Executive Officer, Siemens Canada Limited



Dr. Paul J. Mazerolle
President and Vice-Chancellor, University of New Brunswick



ENDNOTES

- 1 [Responsible Digital Transformation, World Economic Forum 2022.](#)
- 2 [Picking up Speed: Digital Maturity in Canadian SMEs and Why Increasing it Matters, Brookfield Institute \(2021\)](#)
- 3 [Global Information Security Survey, Ernst & Young 2021](#)
- 4 [The Asia Pacific Risk Centre \(Oliver Wyman, Marsh\) 2018](#)
- 5 [APEC Leaders Statement on Counterterrorism \(2001\)](#)
- 6 [2021 Data Breach Investigations Report \(DBIR\), Verizon \(2021\)](#)
- 7 [Cybercrime To Cost the World \\$10.5 Trillion Annually By 2025](#)
- 8 [Cybersecurity threats to cost organizations in Asia Pacific US\\$1.75 trillion in economic losses](#)
- 9 [Fortune Business Insights, 2021](#)
- 10 [Framework for Understanding Cybersecurity Impacts on International Trade, MIT 2019](#)
- 11 [What cybersecurity means for global trade, WEF 2015](#)
- 12 [Global Cybersecurity Outlook, WEF 2022](#)
- 13 [Global Cybersecurity Index, ITU 2020](#)
- 14 [National Cybersecurity Index, e-Governance Academy Foundation 2021](#)
- 15 [Cybersecurity Capacity Maturity Model for Nations \(CMM\), Global Cybersecurity Capacity Centre \(2021\)](#)
- 16 [Cybersecurity Capacity Maturity Model for Nations \(CMM\), Global Cybersecurity Capacity Centre \(2021\)](#)
- 17 [Closing the Digital Skills Gap Report, APEC 2020](#)
- 18 [Global Cybersecurity Outlook, WEF 2022](#)
- 19 [Global Information Security Survey, Ernst & Young 2021](#)
- 20 [Cybersecurity Workforce Study, ISC2 2021](#)
- 21 [Global Information Security Survey, Ernst & Young 2021](#)
- 22 [Global Risks Report, WEF 2022](#)
- 23 [Digital 2022: Global Overview Report, Data Reportal](#)
- 24 [Chart of signatures and ratifications of Treaty 185, Council of Europe](#)
- 25 [2002 APEC Cybersecurity Strategy](#)
- 26 [APEC Cooperative Response Guidelines in Cross-Border Environment, 2008](#)
- 27 [APEC Considerations for Communicating Cybersecurity Practices](#)
- 28 [Global Cybersecurity Outlook, WEF 2022](#)
- 29 [Ibid](#)
- 30 [Ibid](#)
- 31 [Asia-Pacific Cybersecurity Dashboard, BSA The Software Alliance 2015](#)
- 32 [APEC SMEs](#)
- 33 [The Digital Transformation of SMEs, OECD 2021](#)
- 34 [Verizon Data Breach Report 2019](#)
- 35 [60 Percent of Small Companies Close Within 6 Months of Being Hacked, Cybersecurity Ventures 2019](#)
- 36 [Verizon Data Breach Report, Verizon 2022](#)
- 37 [Cybersecurity for Small Businesses: Asia Pacific Businesses Prepare for Digital Défense, CISCO 2021](#)
- 38 [APEC SMEs](#)
- 39 [Digital First Economy: ICT Infrastructure drives economic evolution for sustainable, inclusive growth, ABAC 2022](#)
- 40 [Kergroach, S. \(2021\), "SMEs Going Digital: Policy challenges and recommendations", Going Digital Toolkit Note, No. 15](#)
- 41 [Cloud Computing Adoption in Small and Medium Enterprises \(SMEs\): A Systematic Literature Review and Directions for Future Research, International Journal of Business 2022](#)



APEC Business Advisory Council

