The Software Alliance

BSA

Asia-Pacific Cybersecurity Dashboard

A Path to a Secure Global Cyberspace

galexia

CONTENTS

EXECUTIVE SUMMARY

By adopting the right mix of laws and rules and creating the appropriate institutions and structure that establish clear guidance on cybersecurity, governments can create a sound foundation for taking full advantage of the opportunities of the digital economy and an environment of cooperation with relevant stakeholders. These steps will help all parties involved, from national governments to private-sector actors, in the joint effort that is needed to protect systems and prevent, mitigate and respond to cyber-attacks.

The institutions and the frameworks created to carry out these tasks must be stable and clear. But it is equally important that they remain flexible in order to adjust to the technology world's ever-evolving threat environment.

This study — the inaugural BSA APAC Cybersecurity Dashboard — provides government officials in the 10 markets studied with an opportunity to evaluate their laws, regulations and policies.

The accelerating pace of innovation is evident all around us. From the ever-more powerful microcomputers in our pockets, which we continue to call "phones" only out of habit, to the increasing number of sensor-driven products that populate our daily lives, these advances are revolutionizing almost every sector of the global economy. From agriculture and manufacturing to communications and utilities, software-driven technology is delivering new products and services — as well as benefits — to populations around the world.

An unfortunate parallel to the growing benefits of technology is the growing risk of threats. Hackers and other attackers would take advantage of our increasingly technologically connected world by exploiting vulnerabilities in order to commit crimes or cause major disruption and destruction. This fact makes it vitally important that we ensure the future safety of our cyber-enabled systems by building in resiliencies and a flexibility that will allow evolution.

Governments can help build in bulwarks to cyber-attacks through the cybersecurity policies they adopt and execute. Such policies also can help mitigate the harms of any actual instances of attacks and address emerging threats in the future. To do so, two key elements are indispensable: the proper legal frameworks and the necessary infrastructure to implement them.

This Dashboard focuses on the policies of the markets studied, but the questions that compose the Dashboard also provide a baseline standard by which any country in the region, or around the world, can measure their progress toward a mature cybersecurity policy environment.

The most important takeaways of the Dashboard can be summarized as follows:

- Although the management of cybersecurity is recognized as an important issue in the Asia-Pacific region, the 10 markets included in this study have generally been slow to produce comprehensive national cybersecurity strategies, and to implement the necessary legal frameworks for security and critical infrastructure protection.

In addition to the Dashboard itself, the detailed results of the research are available online — at www.bsa.org/APACcybersecurity

- The opportunity has not been taken to benefit from private-sector experience through formal public-private partnerships in cybersecurity.
- The region has shown strength and consistency in the establishment of computer emergency response teams (CERTs) and the implementation of national cybersecurity education campaigns.
- The imposition of local standards and local testing requirements that are inconsistent with a truly international approach to addressing cybersecurity hampers effective cybersecurity in some markets, notably China, Indonesia and South Korea.

The Dashboard highlights tremendous opportunities to improve cybersecurity throughout the region and identifies shortcomings in the cyber policy environment in certain markets.

The Dashboard examines, in detail, the foundational steps needed to increase cybersecurity and improve cyber resilience. Simply put, policymakers should establish the proper policy, legal and operational frameworks; improve collaboration with various relevant stakeholders' communities; effectively share meaningful cybersecurity information; and prioritize the protection of critical infrastructures. Accomplishing these goals is an urgent matter, and the Dashboard aims to facilitate the discussions and debates needed to advance these interests.

In addition to the Dashboard itself, the detailed results of the research are available online — at **www.bsa.org/APACcybersecurity**. Officials can expand their awareness of the global cyber policy environment by examining the findings of the recently released EU Cybersecurity Dashboard at www.bsa.org/EUcybersecurity.

Because cybersecurity policy evolves almost as quickly as the sector it is intended to govern, the Dashboard also will need to evolve. As national governments and decision makers update their frameworks to address the remaining gaps, this website will be updated to show progress across the relevant areas. We invite you to review these results and contact BSA | The Software Alliance with information regarding any relevant changes.

METHODOLOGY

This study of cybersecurity is based on an assessment of 31 criteria across six themes. Each criteria is given a "Yes," "No," "Partial," or "Not Applicable" status. There are no overall rankings or scores in this study.

This analysis is the result of desk-based research on publicly available information, and did not involve direct interviews with national agencies. Where possible, the research study and summary materials include links to further information and resources.

The research period concluded on 1 January 2015 and general information in the study is correct up to that date. The currency of specific data on ICT infrastructure is noted separately in the study.

A detailed description of the methodology and criteria is available at **www.bsa.org/APACcybersecurity**.

THE BUILDING BLOCKS OF A STRONG LEGAL CYBERSECURITY FRAMEWORK

Construct Solid Legal Foundations

Governments should enact and keep up-to-date a comprehensive legal and policy framework, based on a solid national cybersecurity strategy. This framework should be built upon the following key principles.

- **Risk-based and prioritised:** Cyberthreats come in many shapes and magnitudes with varying degrees of severity. Establishing a hierarchy of priorities — based on an objective assessment of risk — with critical assets and/or critical sectors at the top is an effective starting point from which to ensure that cyber protections are focused on those areas where the potential for harm is greatest.
- **Technology-neutral:** A technology-neutral approach to cybersecurity protection is vital to ensure access to the most secure and effective solutions in the marketplace. Specific requirements or policies that mandate the use of certain technology only undermine security by restricting evolving security controls and best practices, and potentially creating single points of failure.
- **Practicable:** Any strategy is only as effective as it is adoptable by the largest possible group of critical assets, and implementable across the broadest range of critical actors. Overly burdensome government supervision of private operators, or disproportionately intrusive regulatory intervention in their operational management of cybersecurity risk, would most often prove counterproductive, diverting resources from effective and scalable protection to fragmented administrative compliance.
- **Flexible:** Managing cyber risk is a cross-disciplinary function and no "one-size-fits-all" approach exists. Each industry, system and business faces distinct challenges, and the range of actors must have flexibility to address their unique needs.
- **Respectful of privacy and civil liberties:** Security requirements should be duly balanced with the need for protection of privacy and civil liberties. Ensuring that requirements and obligations are proportionate, do not represent more intrusion in fundamental rights than what is strictly necessary, follow due process and are supported by adequate judicial oversight all are important considerations to address in any cybersecurity framework.

Establish Operational Entities with Key Responsibilities for Security

Governments should set up operational entities to support the prevention of cybersecurity incidents and ensure response to them. A core component of this is the establishment of operational computer security, emergency and incident response teams.

Engender Trust and Work in Partnership

No country or government can address cybersecurity risk in isolation. Collaboration with non-governmental entities as well as with international partners and allies is a crucial component of an effective approach to cybersecurity.

- **Partnering with the private sector:** Most infrastructure is owned by the private sector, making effective public-private cooperation essential. Cooperation also improves the effectiveness of risk management by improving the sharing of information, experience and perspective of multiple sources. Particular efforts are needed to foster trust and avoid legal obstacles that may hinder it.
- **Global rather than isolated:** Given that cyberthreats are global, effective cybersecurity policies and strategies need to maintain an international outlook, and build on joint efforts with partners and allies. They should also leverage international, voluntary and market-driven standards in order to maximize pan-regional and global information sharing and protection.

Foster Education and Awareness About Cybersecurity Risk

People, process and technology are equally important to ensuring cybersecurity. Even the best technology will be ineffective if not used appropriately. Awareness raising, education and training about clearly articulated cybersecurity priorities, principles, policies, processes and programs are essential components of any cybersecurity strategy.

INTRODUCTION

Continuing high-profile cybersecurity incidents underline the crucial importance of strengthening cyber resilience in general, as well as the protection of critical infrastructure from cyber threats, both in the Asia-Pacific region and around the world. In order to achieve these goals, public and private stakeholders need to be equipped with the capacity to effectively prevent, mitigate and respond to cyber-attacks and incidents.

With an increasing focus on improving cyber resilience in every market, this study — the inaugural BSA Asia-Pacific Cybersecurity Dashboard — provides a comprehensive overview of the state of the current cybersecurity frameworks and capabilities.

As detailed below, the Dashboard examines the cybersecurity policy environment in 10 Asia-Pacific markets with a focus on five key areas:

- Legal foundations for cybersecurity;
- Operational capabilities;
- Public-private partnerships;
- Sector-specific cybersecurity plans; and
- Education.

In addition, the Dashboard examines a series of other cyberlaw indicators that assess whether the national legal regimes discriminate against, or place unnecessary restrictions or requirements on, global cybersecurity service providers.

LEGAL FOUNDATIONS

Policymakers have a key role to play in ensuring that both public and private entities are well equipped to face the cybersecurity challenges of an ever more connected world. They can achieve this not only by establishing appropriate legal and policy frameworks, but also through promoting cybersecurity awareness and cooperation with the different actors involved in working towards cyber resilience.

A key component, and in many ways the foundation, of this framework is a national cybersecurity strategy, which is critical for managing national level cyber risks and developing appropriate legislation to support those efforts. A strong cybersecurity strategy should be a "living document," developed and implemented in partnership with key public and private stakeholders. It should contain clearly articulated principles and priorities that reflect societal values, traditions and legal principles.

The detailed analysis of the legal frameworks for cybersecurity in these 10 Asia-Pacific markets reveals a broad spectrum of responses. Some markets, notably Australia, India, Japan, Singapore and Taiwan, have detailed and comprehensive cybersecurity strategies in place, often backed up

Policymakers have a key role to play in ensuring that both public and private entities are well equipped to face the cybersecurity challenges of an ever-more connected world.

by legislative and policy instruments that address security, classification and critical infrastructure protection requirements. However, Indonesia has not yet developed a national cybersecurity strategy. The remaining markets — China, Malaysia, South Korea and Vietnam — have implemented some cybersecurity measures, but their national cybersecurity strategies still are being developed.

Governments also should assess and establish clear priorities among the critical services and infrastructures that most need protection. Not all assets, systems, networks, data and services are equally essential. Accordingly, decision makers should assess the national infrastructure and determine those that are providing critical services and functions, whose compromise, damage or destruction through a cybersecurity incident could have national significance.

Once these critical infrastructures are identified, their cyber resilience needs to be evaluated in order to identify and address vulnerabilities and gaps. Best practices developed in the private sector often include systematic internal and third-party audits to test the cyber resilience of critical systems.

Sharing cybersecurity relevant information is no doubt an important aspect of an effective approach to cyber resilience, as it serves the interest of both public and private stakeholders. Judicious information sharing increases collective awareness and, thereby, enables every stakeholder to adapt its security posture to the evolution of the threat landscape.

Effective information sharing, however, requires information protection; appropriate information classification requirements therefore are crucial.

Governments also should facilitate information sharing by supporting the creation of public-private partnerships and sector-specific collaboration. They should also provide the necessary human and technical resources, operational entities and the appropriate legal protections against anti-trust claims, undue disclosure requirements or liabilities. Finally, they should identify and address any other policy and legal barriers that may inhibit information sharing.

OPERATIONAL ENTITIES

Incident-response capabilities should be established to manage the most critical and significant events that threaten the confidentiality, integrity or availability of nationally significant information networks and systems. Computer emergency response teams (CERTs) and computer security incident response teams (CSIRTs) can play a crucial role in improving cyber resilience.

These bodies can provide incident response services to victims of attacks; share information concerning vulnerabilities and threats with key stakeholders in the government, private sector and in some instances with the broader public; and offer other ways of helping improve computer and network security.

All 10 markets in this study of cybersecurity in the Asia-Pacific region have operational CERTs that play an important role in managing cybersecurity incident reporting and responses. Most markets in the study also have engaged in national or regional cybersecurity exercises, and there are only a small number of remaining gaps in the establishment of the operational entities that are necessary for managing cybersecurity.

Effective partnership between public and private sectors is all the more important because non-government entities manage and operate many critical infrastructures we rely on every day, including those that control transportation, health, banking and energy.

PUBLIC-PRIVATE PARTNERSHIP

Effective cybersecurity requires collaboration and coordination among all national stakeholders. Real partnership between public and private sectors is all the more important because non-government entities manage and operate many critical infrastructures we rely on every day, including those that control transportation, health, banking and energy.

The importance of establishing public-private partnerships for cybersecurity is recognized in the Asia-Pacific region, but developments in this field are still at a very early stage. Japan and Malaysia have led the way by establishing formal public-private partnerships for cybersecurity, and there is strong interest in many other markets.

SECTOR-SPECIFIC CYBERSECURITY PLANS

While certain elements of cybersecurity protection apply across all areas, and a wide variety of recommendations are available from national and international organizations, there also is a need for guidance that is tailored to the business needs of particular entities or that provides methods to address unique risks or specific operations in certain sectors.

There is some emerging interest in establishing sector-specific responses to cybersecurity, but implementation in the Asia-Pacific region is very limited. Australia, Malaysia and Singapore are the leaders in this field, and in time other nations may follow with their own sector-specific initiatives.

EDUCATION

No single entity or group of stakeholders can secure cyberspace alone — and no individual or group is without responsibility for playing a part in cybersecurity. Governments and organizations of all sizes, as well as consumers, need to take steps to secure their own systems, education and awareness raising play a crucial role.

This requires educational and awareness-raising campaigns as well as support for the development and generalization of cybersecurity tuition in universities and in earlier curricula.

The Asia-Pacific region has dedicated considerable resources to cybersecurity education, including innovative programs aimed at raising cybersecurity awareness among the general population. A small number of markets, notably Indonesia and Taiwan, are yet to implement national education strategies or programs in this field, but these gaps should be addressed in the near future.

ADDITIONAL CYBERLAW INDICATORS

This study identifies a number of additional cyberlaw settings in the 10 Asia-Pacific markets that may have a negative impact on the management of cybersecurity. These include local requirements that prevent the development and use of appropriate international standards for cybersecurity products and restrictions on the nationality of cybersecurity vendors. They also include unnecessary local testing requirements that are an additional burden on cybersecurity products that have already been tested against international standards.

STUMBLING BLOCKS IN THE PATH TO TRUE SECURITY

Some governments today are invoking cybersecurity as a justification for a variety of policies that go beyond what is needed to address legitimate security concerns. In fact, such policies often undermine cybersecurity rather than improve it. They also impose unfair market access barriers on global producers and service providers, whether intended or not.

Avoid Unnecessary or Unreasonable Requirements

A proper cybersecurity policy enables organizations to develop and adopt the widest possible choice of cutting-edge cybersecurity solutions. It also allows entities to implement the security measures that are most effective at mitigating the specific risks they face.

Some governments instead impose various requirements that restrict choice, increase costs and reduce the ability of their own firms to use the most appropriate cybersecurity tools available. These include, but are not limited to, country-unique certification conditions or local testing requirements; mandates for local content; requirements to disclose sensitive information, such as source codes and encryption keys; and, restrictions on foreign ownership of intellectual property.

Refrain from Manipulating Standards

Technology standards play a vital role in enabling and enhancing cybersecurity. By supporting internationally recognized technical standards that are developed with industry participation and accepted across markets, companies can more quickly develop and distribute newer and more secure products.

Even so, some governments have imposed country-specific standards with the argument that requiring market-specific rules will lead to improved cybersecurity. The real effect, however, is the opposite. Government-imposed standards, rather than bolstering security, tend to freeze innovation and force consumers and businesses into using products that might not suit their needs.

Avoid Data Localization Rules

With the rise of global cloud computing services, companies of all sizes around the world can leverage powerful resources that were once available only to the largest firms. The cloud model, though, is based on networks that allow the storage and processing of data in multiple locations and even in multiple countries. By allowing data to flow freely among multiple markets, cloud providers can deliver numerous advantages, including reliability, resiliency, and 24-hour service support.

Based on the mistaken assumption that data is safer in a specific location, some countries are imposing rules that prohibit or significantly impede data transfers across borders. Policies that unnecessarily restrict the free flow of data undermine the very benefits of cloud computing by increasing costs and threatening to prevent access to emerging cloud-enabled services.

Avoid Preferences for Indigenous Technologies

Cutting-edge products and services are developed through global collaboration in research and design centers in many different countries. Countries should create incentives for cross-border collaboration to facilitate voluntary technology transfer and the rapid development and deployment of enhanced products and services.

However, some countries take the opposite approach, assuming that by preventing foreign competition they can protect domestic champions, develop an indigenous technology industry, and enhance cybersecurity. By definition, indigenous technologies are a subset of global innovation. Preventing foreign competition reduces cybersecurity by denying firms and agencies from buying world-class products and services. Furthermore, such policies deprive domestic technology firms of valuable opportunities to collaborate with global leaders and make them less competitive internationally, harming global innovation.

ASIA-PACIFIC CYBERSECURITY DASHBOARD

✔ Yes ✖ No ◑ Partial

#	QUESTION
	LEGAL FOUNDATIONS
1.	Is there a national cybersecurity strategy in place?
2.	What year was the national cybersecurity strategy adopted?
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?
4.	Is there legislation/policy that requires the establishment of a written information security plan?
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?
6.	Is there legislation/policy that requires security practices/requirements to be mapped to risk levels?
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?
	OPERATIONAL ENTITIES
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?
2.	What year was the computer emergency response team (CERT) established?
3.	Is there a national competent authority for network and information security (NIS)?
4.	Is there an incident-reporting platform for collecting cybersecurity incident data?
5.	Are national cybersecurity exercises conducted?
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?
	PUBLIC-PRIVATE PARTNERSHIPS
1.	Is there a defined public-private partnership (PPP) for cybersecurity?
2.	Is industry organised (i.e., business or industry cybersecurity councils)?
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?
	SECTOR SPECIFIC CYBERSECURITY PLANS
1.	Is there a joint public-private sector plan that addresses cybersecurity?
2.	Have sector-specific security priorities been defined?
3.	Have any sector cybersecurity risk assessments been conducted?
	EDUCATION
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?
	ADDITIONAL CYBERLAW INDICATORS
1.	Are cybersecurity services able to operate free from laws that discriminate based on the nationality of the vendor?
2.	Are cybersecurity services able to operate free from laws or policies that mandate the use of specific technologies?
3.	Are cybersecurity services able to operate free from additional local testing requirements that go beyond international testing requirements?
4.	Are cybersecurity services able to operate free from laws or policies that mandate the submission of source code or other proprietary information?
5.	Are cybersecurity services able to operate free from laws or policies that require service providers to locate their servers inside the subject country?
6.	Are cybersecurity services able to operate free from unnecessary restrictions on cross-border data flows (such as registration requirements)?

Australia	China	India	Indonesia	Japan	Malaysia	Singapore	South Korea	Taiwan	Vietnam
✓	◑	✓	✗	✓	◑	✓	◑	✓	◑
2009	–	2013	–	2013	–	2013	–	2013	–
✓	✓	✓	✗	✓	◑	✓	◑	✓	✗
◑	✗	✗	◑	✓	✗	◑	◑	✗	◑
✓	✓	◑	✓	✓	✓	✓	✓	✓	✓
✓	✓	◑	◑	✓	◑	✓	✓	✓	◑
✗	✗	✗	◑	✗	✗	◑	◑	✓	✗
◑	◑	◑	✗	✗	◑	✗	✗	◑	✗
✓	✗	◑	✗	◑	◑	◑	✗	✓	✗
✓	✗	✓	✗	◑	✗	✗	✗	✗	✗
✓	✗	✓	✗	✓	✓	✓	✓	✓	✗
✓	✗	◑	✗	✓	✓	✓	◑	N/A	N/A
✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2010	2002	2004	2007	1996	1997	1997	1996	1998	2005
✓	◑	✓	✓	✓	✓	✓	✓	✓	✗
✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
◑	✓	✓	✗	✓	✓	◑	✓	✓	✗
✓	✗	◑	✗	◑	✓	✗	◑	✓	✗
✗	✗	◑	◑	✓	✓	✓	◑	◑	◑
◑	◑	✓	◑	✓	◑	◑	◑	◑	✓
✗	✗	◑	✗	✓	–	✗	✗	◑	✗
◑	✗	✗	✗	✗	✓	◑	✗	✗	✗
✗	✗	✗	✗	✗	✗	◑	✗	◑	✗
✗	✗	✗	✗	✗	✗	◑	✗	✗	✗
✓	◑	✓	✗	✓	✓	✓	◑	✓	◑
◑	✗	◑	✗	✓	◑	✓	◑	✓	✗
✓	◑	✓	✓	✓	✓	✓	✓	✓	✗
✓	✗	✗	✗	✓	✓	✓	✗	✓	✓
✓	✗	✓	✗	✓	✓	✓	✓	✓	✓
◑	◑	✓	✗	✓	✓	✓	✓	✓	✗
✓	◑	✓	◑	✓	✓	✓	◑	◑	✓

ESTABLISHING AN APPROPRIATE FRAMEWORK FOR MEANINGFUL CYBER-THREAT INFORMATION SHARING

Cybersecurity incidents or breaches can have a major impact on governments and private entities, as well as individuals. Some high-profile breaches have encouraged governments around the world to consider how to best prevent, detect and react to these incidents.

The exchange and sharing of the appropriate information at the right time — and the coordinated effort among relevant actors that it enables — is considered the best way to reduce and mitigate risks and respond to cyber incidents.

Accordingly, the key question is how to best achieve meaningful and effective information sharing among relevant stakeholders. While some countries have considered mandatory incident notification systems, these alone would not suffice to address the issue of collective awareness and preparedness. When it comes to that, voluntary information exchanges based on trust have proved to be the most efficient way to achieve successful information sharing.

Such meaningful information sharing is not an easy undertaking. It can only be achieved if the necessary environment facilitating such exchanges is in place. Some of the fundamentals of such an environment are the following:

- **Create an environment of trust:** Cyber-threat information sharing, as well as incident reporting, require safeguards and incentives for their effective functioning. These elements help ensure the trust necessary for the operation of such a system. They include guarantees that the sharing of information will not subject the organization providing these to undue liabilities, public humiliation, litigation or sanctions.

- **Ensure a high level of confidentiality:** Given the sensitive nature of the information shared about an incident or cyber threat affecting any critical infrastructure, it is crucial to ensure that confidentiality and security of the communications between the infrastructure operator and any supervisory authorities are respected and maintained, subject to transparent reporting by the authority, as appropriate.

  Nevertheless, in some cases, informing the public of an incident may be necessary. In these instances, all care should be taken to ensure an in-depth dialogue between the entities suffering a breach and the authorities before any disclosure in order to avoid increasing the attack surface, multiplying the impact of the incident, creating panic, or leading to undue public shaming.

- **Ensure reciprocity:** While the private sector owns and operates much of the countries' critical infrastructure, information sharing should not be seen as a one-way provision of relevant data from private to public entities. It should be regarded as a real and mutual exchange of information, based on trust and mutual benefits.

- **Make requirements clear and consistent across jurisdictions:** As mandatory notification requirements cover an ever-increasing number of areas and geographies, the likelihood of facing conflicting legal obligations increases. As various organizations operate in multiple sectors across different countries and regions, the questions of what to report when and to whom already pose important compliance challenges. Therefore, to the extent a mandatory notification system should be introduced, it is imperative to strive for as much consistency as possible not only among the different notification obligations, but also among the various national and regional requirements.

ASIA-PACIFIC CYBERSECURITY MARKET SUMMARIES

The following summaries give an overview of the cybersecurity landscape, based on the set of criteria outlined above, highlighting key cybersecurity legislation and policy, as well as the main entities currently operating within each jurisdiction. For more detailed information on each market surveyed, please refer to the detailed market summaries available at www.bsa.org/APACcybersecurity.

AUSTRALIA

Legal Foundations: Australia's national cybersecurity strategy was adopted in 2009 and is currently under review. A revised strategy is expected to be released in late 2015. While Australia has a strong legal framework for information classification, it enacts its information security through guidelines and similar policy documents as opposed to acts of Parliament, and there is no dedicated information security act or classified information act.

Operational Entities: The Australian Cyber Security Centre, launched in 2014, is a hub bringing together the numerous agencies that are engaged with cybersecurity and information security; however, there remains some confusion regarding the separation of responsibilities. Both CERT Australia and the Australian Signals Directorate operate incident-reporting services.

Public-Private Partnerships: Australia does not have a formal public-private partnership for cybersecurity, however CERT Australia works with the private sector in awareness programs and critical infrastructure protection. The private sector also has been consulted as part of the cybersecurity strategy review process.

Sector-Specific Cybersecurity Plans: There is no joint public-private sector plan in Australia that addresses cybersecurity. The Critical Infrastructure Resilience Strategy does highlight the participation of "sector groups" as a key part of the Trusted Information Sharing Network (TISN), but the TISN was not intended to produce sector-specific plans.

Education: Australia has a comprehensive cybersecurity education strategy in place for all age groups, and has heavily invested in education materials and initiatives.

Additional Cyberlaw Indicators: Australia is largely free of country-specific restrictions on technology providers (e.g., mandatory technology requirements, local testing requirements, and requirements for the sharing of source code), but some restrictions and burdens do exist in the procurement space.

CHINA

Legal Foundations: China does not currently have a national cybersecurity strategy in place, although several government policies include advice on cybersecurity. There is no one specific law that focuses on cybersecurity in China, but there are many provisions under different laws that cover cybersecurity, such as the State Secrets Law 2010.

Operational Entities: China's national CERT, CNCERT/CC. was established in 2002. National information security is handled by a range of different government bodies and there is sometimes very little public information about their operations and objectives.

Public-Private Partnerships: There is little activity regarding public-private partnerships in China in the field of cybersecurity.

Sector-Specific Cybersecurity Plans: There is no joint public-private sector plan in China that addresses cybersecurity.

Education: There is no national cybersecurity education strategy in place in China, but some ad hoc education initiatives have been undertaken by the CERT and the Ministry of Industry and Information Technology.

Additional Cyberlaw Indicators: China imposes a range of legal and policy restrictions on cybersecurity service providers.

INDIA

Legal Foundations: India's National Cyber Security Policy was adopted in 2013. It is a detailed plan that includes both high-level principles and targeted objectives and proposals. However, the plan has not been fully implemented and the legal framework supporting cybersecurity remains weak.

Operational Entities: CERT-In, the national CERT, is involved in high-level policy discussions related to information security.

Public-Private Partnerships: Private-sector representative bodies in India are well developed and proactive with regard to cybersecurity. CERT-In also liaises with the private sector; however, there is no dedicated public-private partnership.

Sector-Specific Cybersecurity Plans: There is no joint public-private sector plan that addresses cybersecurity in India. A Joint Working Group has been established to discuss and present recommendations on public-private partnerships in cybersecurity. The working group includes industry representatives.

Education: Creating a culture of cybersecurity awareness through a series of promotional activities and education initiatives is one objective of the Indian National Cyber Security Policy 2013, which also includes a commitment to a comprehensive national awareness raising campaign on cybersecurity.

Additional Cyberlaw Indicators: India has avoided several legal and policy burdens on cybersecurity providers, but it continue to impose local testing requirements in addition to international testing regimes.

INDONESIA

Legal Foundations: Indonesia is in the early stages of developing a national cybersecurity strategy. The legal framework for cybersecurity in Indonesia is weak. There is no clear classified security law or policy, and security practices are spread across different legislation. There are no specific cybersecurity provisions in place.

Operational Entities: ID.SIRTII/CC, the national CERT, seems to be in the early phases of operation. ID.CERT is a non-government CERT, but has been operating for longer.

Public-Private Partnerships: There is no dedicated cybersecurity public private partnership in Indonesia, so the CERT acts as the main liaison body for the private sector. Industry representative associations exist, but none are dedicated to cybersecurity in particular.

Sector-Specific Cybersecurity Plans: Indonesia lacks any joint public-private sector plan to address cybersecurity.

Education: Indonesia lacks a cybersecurity education strategy.

Additional Cyberlaw Indicators: Indonesia subjects cybersecurity service providers to a range of burdensome laws and policies, including discriminatory procurement preferences, local testing requirements, and limits on data flows.

JAPAN

Legal Foundations: Japan's Cybersecurity Strategy, adopted in 2013, is a comprehensive document that identifies not only proposed measures, but also address the roles of various stakeholders with regard to Japanese cybersecurity. The legal framework supporting cybersecurity is one of the strongest in the region, following the recent passage of the Basic Law on Cybersecurity 2014. Japan also passed a new state secrets law in December 2013 that imposes much stronger security practices on the handling of sensitive information and stronger penalties in cases of unauthorised access.

Operational Entities: The operational entities in Japan that relate to cybersecurity are all mature. The national cert, JCERT/CC, was established in 1996 and maintains a strong web presence. The Cyber Security Strategy Headquarters has also been established under the Basic Law on Cybersecurity 2014.

Public-Private Partnerships: Japan has a mature public-private partnership structure for cybersecurity, including J-CSIP, whose members include representatives from government and private entities involved with critical national infrastructure.

Sector-Specific Cybersecurity Plans: There is no joint public-private sector plan in Japan that addresses cybersecurity.

Education: Japan's Cybersecurity Strategy 2013 contains a detailed and comprehensive commitment to educating young people about cybersecurity.

Additional Cyberlaw Indicators: Japan avoids undue legal and regulatory restrictions on cybersecurity service providers.

MALAYSIA

Legal Foundations: Malaysia does not have a single cybersecurity strategy, but refers to its collection of policies and strategies as Malaysia's Cyber Security Policy. The Malaysian Government has announced that this suite of policies will be completely revised and strengthened by 2017.

Operational Entities: CyberSecurity Malaysia runs the national cert — MyCert — as well as the reporting service Cyber999. It also acts as the chief authority on information security.

Public-Private Partnerships: CyberSecurity Malaysia organizes an awards event which doubles as an annual convention on cyber security in a public-private partnership model.

Sector-Specific Cybersecurity Plans: Public-private cooperation is a key principle of Malaysia's National Cyber Security Policy, which uses a sector-based approach to address security concerns and identifies 10 critical sectors for this purpose.

Education: The Cybersafe program provides a comprehensive suite of materials and activities relating to cybersecurity.

Additional Cyberlaw Indicators: Malaysia's government procurement regime includes certain restrictions on global cybersecurity providers, but the country otherwise avoids many undue legal and regulatory burdens.

SINGAPORE

Legal Foundations: Singapore adopted a five-year National Cyber Security Masterplan in 2013, and also is continuing to develop its critical infrastructure protection regime. Singapore has some broad legal infrastructure in place for cybersecurity. The new Singapore Cybersecurity Agency will begin operations in April 2015.

Operational Entities: SingCERT was established as the national computer emergency response team in 1997, and the Infocomm Development Authority (IDA) acts as a high-profile coordinating agency for all aspects of information communications policy, including cybersecurity.

Public-Private Partnerships: Singapore's government agencies work closely with the private sector in the field of cybersecurity, and there is a formal commitment to the development of public-private partnerships.

Sector-Specific Cybersecurity Plans: The Infocomm Security Masterplan 2 (MP2), launched in 2008, stated the Singapore government would work to develop sector-specific security programs, particular with regard to owners of critical infrastructure. MP2 has been subsequently succeeded by a plan that, although building on MP2, does not include a direct commitment to the sector-based programs.

Education: The National Cyber Security Masterplan 2018, published in 2013, includes a strong commitment to cybersecurity education.

Additional Cyberlaw Indicators: Singapore avoids undue legal and regulatory restrictions on cybersecurity service providers.

SOUTH KOREA

Legal Foundations: South Korea takes a national security and defense-focused approach to cybersecurity. As such, the country's Cyber Security Master Plan, issued in 2011, is more a cyberdefense strategy than a cybersecurity strategy. There are some minor gaps in their legal framework.

Operational Entities: Both KrCERT/CC and KN-CERT (government only) are established computer emergency response teams. Information security responsibilities are centralized in the Korea Internet and Security Agency, which has a considerable online presence.

Public-Private Partnerships: KrCERT/CC liaises with the private sector as part of its incident response duties; however, there is no formal public private partnership for cyber or information security in South Korea.

Sector-Specific Cybersecurity Plans: There is no joint public-private sector plan in South Korea that addresses cybersecurity.

Education: The Korea Information Security Agency is responsible for promoting the responsible use of the internet among users, and the agency conducts a range of online and broadcast awareness-raising campaigns.

Additional Cyberlaw Indicators: South Korea places certain undue restrictions on cybersecurity service providers, including Korea-specific testing rules.

TAIWAN

Legal Foundations: Taiwan's National Information and Communication Security Taskforce has developed several National Information Security Policy and Strategy documents. The current strategy covers the period from 2013 to 2016.

Operational Entities: Taiwan has two computer emergency response teams in place and collectively they cover cybersecurity incidents across the Taiwanese network. Government responsibility for network information and security rests within the Ministry for National Defense.

Public-Private Partnerships: While there is no defined public-private partnership in Taiwan for cybersecurity, the CERT does closely liaise with the private sector.

Sector-Specific Cybersecurity Plans: There is no joint public-private sector plan in Taiwan that addresses cybersecurity.

Education: Cybersecurity education is coordinated by the National Information and Communication Security Taskforce. The Ministry of Education has also developed a cybersecurity education website.

Additional Cyberlaw Indicators: Taiwan avoids most undue restrictions on cybersecurity service providers, but it does allow for the restriction of certain cross-border data flows.

VIETNAM

Legal Foundations: There is no national cybersecurity strategy in place in Vietnam, although the 2012-2015 National Anti-Crime Master Plan does include some very limited coverage of cybercrime. The legal infrastructure for critical infrastructure protection in Vietnam also is limited. A draft Law on Information Security will lead to improvements in this field if it is enacted.

Operational Entities: VNCERT, the national computer emergency response team, was established in 2005. Other operational entities in Vietnam are quite limited; however, these gaps may be addressed by proposals in the draft Law on Information Security.

Public-Private Partnerships: While Vietnam does not have a defined public-private partnership for cybersecurity, VNCERT liaises closely with the private sector.

Sector-Specific Cybersecurity Plans: There is no joint public private-sector plan in Vietnam that addresses cybersecurity.

Education: Vietnam has introduced some technical training and education courses for cybersecurity capacity building, but there is no general public awareness campaign or education strategy.

Additional Cyberlaw Indicators: Vietnam imposes certain procurement restrictions and technology mandates on cybersecurity service providers.

ABOUT BSA

BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life.

With headquarters in Washington, DC, and operations in more than 60 countries around the world, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

ABOUT GALEXIA

Galexia (www.galexia.com) is at the forefront of international research and advice in the areas of privacy, identity, cybersecurity and cloud — with a particular focus on global and cross-border legal and regulatory issues. We have expertise in the policy complexities that arise for countries addressing cybersecurity issues. We provide advice on national cybersecurity strategies, critical infrastructure protection and the establishment of cybersecurity management and alert systems.

We work closely with a diverse range of international, business and government clients to produce clear and effective outcomes from evidence based research. We utilise collaborative cloud based reporting tools to provide real time access to our research and analysis.

The Software Alliance

BSA

www.bsa.org

BSA Worldwide Headquarters

20 F Street, NW
Suite 800
Washington, DC 20001

T: +1.202.872.5500
F: +1.202.872.5501

BSA Asia-Pacific

300 Beach Road
#25-08 The Concourse
Singapore 199555

T: +65.6292.2072
F: +65.6292.6369

BSA Europe, Middle East & Africa

2 Queen Anne's Gate Buildings
Dartmouth Street
London, SW1H 9BP
United Kingdom

T: +44.207.340.6080
F: +44.207.340.6090