BSA The Software Alliance

COUNTRY: **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.

QUESTION	RESPONSE	EXPLANATORY TEXT
LEGAL FOUNDATIONS		
1. Is there a national cybersecurity strategy in place?	◑	There is no discrete cybersecurity strategy in place in Vietnam. Vietnam does have a 2012–2015 National Anti-Crime Master Plan, issued by the Prime Minister in 2012, which includes a sub-plan specifically on anti-cybercrime. The Plan allocates resources for local police forces to develop the capacity to investigate cybercrime. Some resources also point to the development of a National Master Plan to Secure Cyber-Space for the Period from 2010 to 2020. However, this document is not available to the public as of May 2015.
2. What year was the national cybersecurity strategy adopted?	–	
3. Is there a critical infrastructure protection (CIP) strategy or plan in place?	✖	There is no discrete critical infrastructure protection strategy in place in Vietnam. The Joint Circular on Assurance of Infrastructure Safety and Information Technology in Post, Telecommunications and Information Technology Activities 2008 <english.mic.gov.vn/vbqppl/Lists/Vn%20bn%20QPPL/DispForm.aspx?ID=6326> addresses information technology infrastructure, in passing, but does not define or address critical infrastructure.
4. Is there legislation/policy that requires the establishment of a written information security plan?	◑	There is no legislation in place in Vietnam that requires the establishment of a written information security plan. A draft Information Security Law <duthaoonline.quochoi.vn/DuThao/Lists/DT_DUTHAO_LUAT/View_Detail.aspx?ItemID=655&LanID=656&TabIndex=1> details extensive practices, regulations, and requirements related to information security and the protection of information systems, including expanding the responsibilities and capabilities of government agencies such as VNCERT. The draft law is proposed to be presented to the parliament of Vietnam in 2015 and take effect from 2016. Pursuant to multiple relevant laws, including the National Security Law 2004 and the Law on Information and Technology 2006, the Ministry of Information and Security and the Ministry of Public Security jointly issued the Circular on Assurance of Infrastructure Safety and Information Technology in Post, Telecommunications and Information Technology Activities <english.mic.gov.vn/vbqppl/Lists/Vn%20bn%20QPPL/DispForm.aspx?ID=6326>. This is circular details the assurances and requirements in Vietnamese law that concern information security.

COUNTRY: VIETNAM

QUESTION	RESPONSE	EXPLANATORY TEXT
5. Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✓	The Ordinance on State Secrets Protection 2000 <www.moj.gov.vn/vbpq/en/Lists/Vn%20bn%20php%20lut/View_Detail.aspx?ItemID=4> requires information covering politics, national defense, security, external affairs, and science and technology to be classified. Chapter II of the ordinance details a three-tiered classification system for the classified information. Classification levels are assigned according to the contents of the information.
6. Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels?	◑	The Ordinance on State Secrets Protection 2000 <www.moj.gov.vn/vbpq/en/Lists/Vn%20bn%20php%20lut/View_Detail.aspx?ItemID=4> outlines practices for handling state secrets, however these are general and limited, and not mapped to either classification levels or risk levels. Some security practices, related to information technology in particular, are detailed in the Joint Circular on Assurance of Infrastructure Safety and Information Technology in Post, Telecommunications and Information Technology Activities 2008, however, these practices do not map to risk levels.
7. Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✗	There is no legislation in place in Vietnam that requires an annual cybersecurity audit. The draft Law on Information Security <duthaoonline.quochoi.vn/DuThao/Lists/DT_DUTHAO_LUAT/View_Detail.aspx?ItemID=655&LanID=656&TabIndex=1> requires information security audits to be carried out by the Ministries of Justice, Defense, and Information and Communications. It does not detail the audit process nor specify a required frequency.
8. Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	✗	There is no legislation in place in Vietnam 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)?	✗	There is no legislation in place in Vietnam that requires each agency to have a chief information officer or chief security officer.
10. Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✗	The draft Law on Information Security requires incidents detected by organizations to be reported to the competent authority. The draft law will be introduced to the parliament of Vietnam in 2015 and take effect from 2016.
11. Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✗	There is no legislation or policy in place in Vietnam that includes an appropriate definition for "critical infrastructure protection".
12. Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	Not applicable	There are no specific cybersecurity standards or certification requirements for procurement in Vietnam, as of May 2015.
OPERATIONAL ENTITIES		
1. Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✓	VNCERT <vncert.gov.vn> was established in 2005. It assists with cyber incident response measures for all incidents affecting .vn domain hosts and those addresses assigned to Vietnamese ISPs.
2. What year was the computer emergency response team (CERT) established?	2005	
3. Is there a national competent authority for network and information security (NIS)?	✗	There is no national competent authority for network and information security in Vietnam. The responsibility for network and information security is shared by the Ministries of Information and Communications, Public Security and Defense. The draft Law on Information Security makes reference to a competent authority, though such an agency is not identified by name. The draft law will be introduced to the parliament of Vietnam in 2015 and take effect in 2016.
4. Is there an incident-reporting platform for collecting cybersecurity incident data?	✓	VNCERT <vncert.gov.vn> provides an online form and email-based incident-reporting platform to log cybersecurity incidents.
5. Are national cybersecurity exercises conducted?	✗	National cybersecurity exercises are not conducted in Vietnam.

COUNTRY: VIETNAM

QUESTION	RESPONSE	EXPLANATORY TEXT
6. Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✖	There is no national incident management structure in place in Vietnam. The draft Law on Information Security requires the establishment of a national Emergency Response Plan and the issuing by the Prime Minister of other contingency plans. The draft law will be introduced to the parliament of Vietnam in 2015 and will take effect from 2016.
PUBLIC-PRIVATE PARTNERSHIPS		
1. Is there a defined public-private partnership (PPP) for cybersecurity?	◑	While Vietnam does not have a defined public-private partnership for cybersecurity, VNCERT <www.vncert.gov.vn> liaises with the private sector in order to implement and coordinate incident response procedures.
2. Is industry organized (i.e., business or industry cybersecurity councils)?	✔	The Vietnam Information Security Association (VNISA) <www.vnisa.org.vn> is an industry-led organization that promotes the development and implementation of information security best practices in Vietnam.
3. Are new public-private partnerships in planning or underway (if so, which focus area)?	✖	As of May 2015, there are no documented new public-private partnerships being planned in Vietnam.
SECTOR-SPECIFIC CYBERSECURITY PLANS		
1. Is there a joint public-private sector plan that addresses cybersecurity?	✖	There is no joint public-private sector plan in Vietnam that addresses cybersecurity.
2. Have sector-specific security priorities been defined?	✖	Sector-specific security priorities have not been publicly defined.
3. Have any sector cybersecurity risk assessments been conducted?	✖	Sector cybersecurity risk assessments have not been conducted in Vietnam.
EDUCATION		
1. Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	◑	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		
1. Are cybersecurity services able to operate free from laws that discriminate based on the nationality of the vendor?	✖	The 20 April 2010 Prime Minister's Directive on Public Procurement states that international bids will only be invited when local goods and equipment cannot meet the requirements of a tender. In 2012, Vietnam became an observer to the WTO plurilateral Agreement on Government Procurement, but is not yet a full member.
2. Are cybersecurity services able to operate free from laws or policies that mandate the use of specific technologies?	✖	In 2009 the Vietnam Minister of Information and Communications announced that it was mandatory that "100% of clients of IT divisions of government agencies must be installed with open source software". Note that a lower limit (70%) applied to non-IT agencies.
3. Are cybersecurity services able to operate free from additional local testing requirements that go beyond international testing requirements?	✔	There are no local testing requirements for cybersecurity services, as of May 2015.
4. Are cybersecurity services able to operate free from laws or policies that mandate the submission of source code or other proprietary information?	✔	There are no requirements for cybersecurity services to submit source code, as of May 2015.
5. Are cybersecurity services able to operate free from laws or policies that require service providers to locate their servers inside the subject country?	✖	Vietnam's Decree 72 on the management, provision and use of Internet services and online information, 2013, <english.mic.gov.vn/vbqppl/Lists/Vn%20bn%20QPPL/DispForm.aspx?ID=6394> requires most internet services to register under Vietnam's telecommunications regulatory regime. This regime requires service companies to operate at least one data center in Vietnam.
6. Are cybersecurity services able to operate free from unnecessary restrictions on cross-border data flows (such as registration requirements)?	✔	There are no registration requirements or other unnecessary restrictions on cross-border data flows in Vietnam.