# Report of the ICC and CICTE: Survey of cyber security and CERT capacity in the Americas

Joseph Richardson
Ajay Nagarajan
Arun Sood

March 2011

International Cyber Center
George Mason University
4400 University Dr, MS 4A5
Voice: 703-993-1524 / 1530
Fax: 703-993-1710

CO-SPONSORS

Organización de los Estados Americanos

The International Cyber Center (ICC) at George Mason University and the Inter-American Committee on Terrorism (CICTE) of the Organization of American States (OAS) conducted a survey to determine the current state of cyber security and CERT capacity in the countries of the Americas. This survey was intended to establish a baseline on progress made and to promote understanding of the needs and requirements of the region going forward. The results of the survey can be fount on the ICC and CICTE websites.

The survey was conducted during the fourth quarter of 2010. A total of 50 valid responses were received representing 20 countries of the Americas. Of those responding, 43 (86 percent) identified themselves as government employees, 3 (6%) as from the private sector and 4 (8%) from Academia. None came from civil society.

The survey was divided into three parts. Part one dealt with national incident management capability and sought information on functions related to incident management being performed within the country. Part two addressed issues of legal infrastructure and sought information on actions taken to address cybercrime and other legal authorities. Part three addressed the development of a national strategy for cyber security and sought information on actions taken to provide a national policy framework for cyber security.

**Part 1: National Incident Management Capability**

The survey identified 23 functions associated with cyber incident management (see annex 1) and asked whether these functions were currently being performed within the country. These 23 functions are often associated with the activities of a CERT with national responsibility (N-CERT) and the questionnaire asked whether an N-CERT had been established within the country.

Based on the responses, the average country of the Americas is currently addressing 9.2 (40 %) of the 23 functions associated with cyber incident management. Twenty-four respondents (48 %) report their country has established a CERT with national responsibilities (N-CERT). For countries with an N-CERT respondents report an average of 11.5 of the 23-cyber incident management functions are being performed. Meanwhile, for countries without an N-CERT respondents their report an average of 7 (30 %) of the activities associated with cyber incident management are being performed.

Looking at the individual functions, the level of activity reported varies widely, as low as 8 (16 %) for function “O” (Coordinating the government’s response to and recovery from large-scale cyber attacks) and as high as 30 (60 %) for function ‘M” (Participating in international cyber security cooperative and information sharing activities.)

Four of the functions (B, C, M and R) were reported as underway in their country by 50 percent or more of respondents.

B. Analyzing cyber threats and vulnerabilities and disseminating cyber threat warning information. (54 %)
C. Analyzing and synthesizing cyber incident and vulnerability information disseminated by others, including vendors and technology experts to provide an assessment for interested stakeholders. (52 %)
M. Participating in international cyber security cooperative and information sharing activities. (60 %)
R. Developing and implementing cyber security awareness programs and initiatives for users of systems and networks. (56 %)

An additional eight functions (A, D, E, I, J, L, N, T, and W) were reported by 40 percent or more of respondents as being performed in their country.

A. Detecting and identifying anomalous activity within the national cyber network. (48 %)
D. Establishing trusted communications mechanisms and facilitating communications among stakeholders to share cyber information and address cyber security issues; providing early warning information, including information about mitigating vulnerabilities and potential problems. (48 %)
E. Developing mitigation and response strategies and effecting a coordinated response to cyber incidents. (40 %)
I. Publicizing general cyber security best practices and guidance for incident response and prevention. (46 %)
J. Leading mechanism(s) within government for coordination among government ministries and agencies to prepare for, detect, respond to, and recover from national cyber incidents. (44 %)
L. Maintaining points of contact network(s) within government agencies, the private sector and international partners to facilitate consultation, cooperation, and information exchange regarding cyber incidents. (42 %)
N. Developing tools and procedures for the protection of the cyber resources of government entities. (42 %)
T. Providing outreach to civil society with special attention to the needs of children and youths, persons with disabilities, and individual users regarding cyber security and their roles. (40 %)
W. Reviewing existing legal infrastructures and updating them to the online environment. (46 %)

The full list is shown in Annex 1.

**Part 2: Legal Infrastructure:**

The establishment and modernization of criminal law, procedures, and policy and the review for adequacy of other legal authorities are necessary to support an effective cyber security/CIIP effort. This requires the development, enactment and enforcement of a comprehensive set of laws relating to cyber-security and cybercrime. The survey sought information on the level of national activity related to cyber crime and the identification of other legal infrastructures related to cyber security that are being addressed.

Concerning cyber crime, the survey identified six key activities related to the modernization of criminal law, procedures and policy and asked respondents to estimate the extent of action within their country in each area using a scale of 0 to 5, with 0 being no activity and 5 being a completed activity. The activities identified were:

A. Establish and adopt substantive, procedural and mutual assistance laws and policies to address cybercrime.
B. Establish or identify national cybercrime units.
C. Develop cooperative relationships with other elements of the government cyber security infrastructure to address cybercrime.
D. Develop cooperative relationships with the private sector to address cybercrime.
E. Develop an understanding among prosecutors, judges, and legislators of cybercrime issues.
F. Participate in the 24/7 Cybercrime Point of Contact Network.

For each of the six activities, one third or more of respondents reported no activity in their country related these cyber crime modernizations. When combined with those reporting low levels of activity (levels 1 and 2) over 80 % of respondents report no or only low levels of activity related to the development of the cybercrime legal infrastructure. At the other end of the activity scale, an average of 8 % of respondents report these activities as completed or nearly completed.

| | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| A. Establish and adopt substantive, procedural and mutual assistance laws and policies to address cybercrime. | 34% | 12% | 20% | 20% | 8% | 6% |
| B. Establish or identify national cybercrime units. | 36% | 22% | 10% | 18% | 8% | 6% |
| C. Develop cooperative relationships with other elements of the government | 36% | 26% | 22% | 6% | 4% | 6% |

| | | | | | | |
|---|---|---|---|---|---|---|
| **cyber security infrastructure to address cybercrime.** | | | | | | |
| **D. Develop cooperative relationships with the private sector to address cybercrime.** | **42%** | **24%** | **24%** | **6%** | **0%** | **4%** |
| **E. Develop an understanding among prosecutors, judges, and legislators of cybercrime issues.** | **34%** | **28%** | **22%** | **10%** | **0%** | **6%** |
| **F. Participate in the 24/7 Cybercrime Point of Contact Network.** | **36%** | **34%** | **16%** | **4%** | **4%** | **6%** |
| **Average** | **36%** | **24%** | **19%** | **11%** | **4%** | **6%** |

The survey also identified 5 other legal infrastructures that support cyber security and asked the status of review and modernization of each in respondents' country. Only Date Protection at 59 % exceeded the half way mark. Commercial Law and Encryption at 14 % each were notably low, while 22 % of respondents reported no activity on any of these legal infrastructures in their country.

| | Number | % of total |
|---|---|---|
| Privacy | 16 | 32 % |
| Data protection | 31 | 62 % |
| Commercial Law | 8 | 16 % |
| Digital signatures | 23 | 46 % |
| Encryption | 7 | 14 % |
| None of the above | 11 | 22% |

**Part 3: National Strategy**

The final section of the survey dealt with the development of a national cyber security strategy as a policy or vision statement to raise awareness of cyber issues among all involved stakeholders and to coordinate a national response to cyber security.

The survey sought information on whether the nations of the Americas had adopted a national strategy, and if so, what were its contents. The survey identified 17 objectives often included in a national cyber security strategy (see annex 2) and sought information on whether these objectives were included in the national cyber strategy of the respondent's home country. For countries without a national cyber

strategy, the respondents were asked to identify which if any of the 17 objectives were the subject of national objectives outside a national cyber strategy.

Of the 50 respondents to the survey, 11 (22 %) reported their country had adopted a national cyber security strategy and 39 (78 %) reported their country did not have a national cyber security strategy. Respondents reported that on average the countries of the Americas, including those with and without a national cyber strategy, are addressing 5 (29 %) of the 17 objectives.

Within this average, 11 (22 %) of respondents reported their country is addressing none of the 17 objectives. For those countries reported as having a national cyber strategy, the nation is reported as addressing an average of 10.7 (63 %) of the 17 objectives. Meanwhile for those nations reported as without a national cyber security strategy respondents reported these countries were addressing only 3.5 (20 %) of the 17 objectives.

The frequency with which individual cyber objectives were reported, both for countries with and national cyber strategy and those without an national cyber strategy is provided in annex 2.

**Conclusions:**

The sample size is small and detailed conclusions are difficult. However, some broad conclusions with implications for cyber security policy within the OAS and the countries of the Americas can be drawn. The survey supports the idea that efforts are underway in most all countries of the Americas to address cyber security and thus there is a base of cyber security expertise upon which to build a more vigorous and comprehensive response. Activities underway include those associated with national incident management and the operations of a CERT with national responsibilities (N-CERT), and those associated with adjustment to the legal infrastructure to respond to cyber crime and other legal issues. The survey also supports the idea that the existence of a national organization to coordinate cyber management (N-CERT) and a national cyber security strategy to organize the national response to cyber security are important elements of a more comprehensive national cyber security effort.

Annex 1

**Potential Functions of a National Incident Management Capability**

| | | Percentage reporting their nation does this activity: |
|---|---|---|
| A. | Detecting and identifying anomalous activity within the national cyber network. | 48 % |
| B. | Analyzing cyber threats and vulnerabilities and disseminating cyber threat warning information. | 54 % |
| C. | Analyzing and synthesizing cyber incident and vulnerability information disseminated by others, including vendors and technology experts to provide an assessment for interested stakeholders. | 52 % |
| D. | Establishing trusted communications mechanisms and facilitating communications among stakeholders to share cyber information and address cyber security issues; providing early warning information, including information about mitigating vulnerabilities and potential problems. | 48 % |
| E. | Developing mitigation and response strategies and effecting a coordinated response to cyber incidents. | 40 % |
| F. | Sharing data and information about cyber incidents and corresponding responses among domestic government and private sector entities. | 32 % |
| G. | Sharing data and information about cyber incidents and corresponding responses among regional and international government and private sector entities. | 30 % |
| H. | Tracking and monitoring cyber information to determine trends and long term remediation strategies. | 32 % |
| I. | Publicizing general cyber security best practices and guidance for incident response and prevention. | 46 % |
| J. | Leading mechanism(s) within government for coordination among government ministries and agencies to prepare for, detect, respond to, and recover from national cyber incidents. | 44 % |
| K. | Leading collaborative relationships with the private sector to prepare for, detect, respond to, and recover from national cyber incidents. | 30 % |
| L. | Maintaining points of contact network(s) within government agencies, the private sector and international partners to facilitate consultation, cooperation, and information exchange regarding cyber incidents. | 42 % |
| M. | Participating in international cyber security cooperative and information sharing activities. | 60 % |

| | | |
|---|---|---|
| N. | Developing tools and procedures for the protection of the cyber resources of government entities. | 42 % |
| O. | Coordinating the government's response to and recovery from large-scale cyber attacks. | 16 % |
| P. | Promoting responsible disclosure practices to protect operations and the integrity of the cyber infrastructure. | 32 % |
| Q. | Developing and implementing a cyber-security plan for government-operated systems. | 38 % |
| R. | Developing and implementing cyber security awareness programs and initiatives for users of systems and networks. | 56 % |
| S. | Encouraging and cooperating with industry on the development and implementation of a culture of cyber security in business enterprises. | 28 % |
| T. | Providing outreach to civil society with special attention to the needs of children and youths, persons with disabilities, and individual users regarding cyber security and their roles. | 40 % |
| U. | Promoting a comprehensive national awareness program so that all participants—businesses, the general workforce, and the general population—secure their own parts of cyberspace. | 26 % |
| V. | Enhancing Science and Technology (S&T) and Research and Development (R&D) related to cyber security. | 38 % |
| W. | Reviewing existing legal infrastructures and updating them to the online environment. | 46 % |

Annex 2

| **Objectives Associated with a National Cyber Security Strategy** | Percentage reporting With Cyber Strategy | Without Cyber Strategy |
|---|---|---|
| 1. Establish national vision/goals for cyber security. | 100 % | 15 % |
| 2. Establish national vision/goals for the protection of critical infrastructures, including critical information infrastructures. | 73 % | 18 % |
| 3. Establish mechanism for coordination among government agencies on the development, monitoring and addressing of cyber security policy issues. | 73 % | 18 % |
| 4. Provide for the solicitation and inclusion of industry views in the development of cyber security policy. | 64 % | 8 % |
| 5. Establish mechanism for coordination among government agencies for operational and incident management issues related to cyber security. | 82 % | 23 % |
| 6. Establish mechanism for cooperation between government and industry on operational and incident management issues related to cyber incident management. | 64 % | 10 % |
| 7. Establish mechanism to facilitate cooperation and information sharing among private sector entities, including critical industries, related to cyber security. | 64 % | 8 % |
| 8. Create a national cyber incident management capability. | 64 % | 20 % |
| 9. Establish a computer security incident response team with national responsibilities (N-CERT). | 55 % | 28 % |
| 10. Review adequacy of existing legal infrastructure in the information age. | 45 % | 28 % |
| 11. Address cybercrime. | 64 % | 41 % |
| 12. Expand ICT infrastructure to an increased portion of the population. | 64 % | 31 % |
| 13. Outreach to citizens and small business to address their cyber security issues. | 45 % | 13 % |
| 14. Protect and enhance investment in ICT infrastructure. | 36 % | 18 % |
| 15. Provide education and training on ICTs and cyber security. | 82 % | 28 % |
| 16. Research and development in cyber security. | 45 % | 10 % |
| 17. Enhance international cooperation in cyber security. | 55 % | 36 % |