BSA The Software Alliance

# COUNTRY: **CROATIA**

Croatia has yet to establish a comprehensive cybersecurity strategy or a well-developed system of public-private partnerships.

Croatia has two established computer emergency response teams (CERTs). The National CERT, established in 2009 is responsible for coordinating security and incident response measures for parties that use a Croatian IP address or .hr domain. The Information Systems Security Bureau's ZSIS CERT has jurisdiction over Croatian government institutions.

| QUESTION | RESPONSE | EXPLANATORY TEXT |
|---|---|---|
| **LEGAL FOUNDATIONS** | | |
| 1. Is there a national cybersecurity strategy in place? | ✖ | Croatia does not have a national cybersecurity strategy in place.<br>Measures concerning cybersecurity capacity are addressed, in part, in the Security and Intelligence System Act 2006. <www.zsis.hr/UserDocsImages/Sigurnost/Security/Security%20and%20Intelligence%20System%20Act.pdf><br>The Security and Intelligence System Act assigns duties to various security and intelligence agencies with regards to cybersecurity and also includes protocols on implementation and regulation. As a strategic security document, the act only addresses cybersecurity as it relates to national defence. |
| 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 critical infrastructure protection (CIP) strategy or plan in Croatia. |
| 4. Is there legislation/policy that requires the establishment of a written information security plan? | ✖ | As of August 2014, there is no legislation/policy in place in Croatia that requires a written information security plan. |
| 5. Is there legislation/policy that requires an inventory of "systems" and the classification of data? | ✔ | Act on Information Security <www.soa.hr/UserFiles/File/information_security.pdf> requires sensitive information to be classified by a three-tiered classification system, as set out in the act. The classification levels are assigned according to the level of risk involved in disclosing the classified information.<br>The Data Secrecy Act 2006 <www.zakon.hr/z/217/Zakon-o-tajnosti-podataka> and the Data Protection Act 1996 <narodne-novine.nn.hr/clanci/sluzbeni/265580.html> requires the classification of government data with regards to its disclosure status. |
| 6. Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels? | ✔ | Section 7 of the Regulation on Information Security Measures 2008 <narodne-novine.nn.hr/clanci/sluzbeni/339036.html>, pursuant to Article 7 of the Act on Information Security 2007 <www.soa.hr/UserFiles/File/information_security.pdf>, requires a continuous process of risk assessment for classified information, which determines the appropriate degree of the security measures applied. |
| 7. Is there legislation/policy that requires (at least) an annual cybersecurity audit? | ✖ | As of August 2014, there is no legislation or formal requirement to conduct an annual cybersecurity audit in Croatia. |
| 8. Is there legislation/policy that requires a public report on cybersecurity capacity for the government? | ◑ | Section 8 of the Regulation on Information Security Measures 2008 <narodne-novine.nn.hr/clanci/sluzbeni/339036.html>, pursuant to Article 7 of the Act on Information Security 2007 <www.soa.hr/UserFiles/File/information_security.pdf>, requires the Office of the National Security Council to monitor the implementation of information security measures, and to provide in writing the subsequent findings to the head of the body or entity into which the monitoring was conducted. There is no requirement for these findings to be published publicly. |
| 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 or policy in place in Croatia that requires each agency to have a chief information officer or chief security officer. |

COUNTRY: CROATIA

| | QUESTION | RESPONSE | EXPLANATORY TEXT |
|---|---|---|---|
| 10. | Is there legislation/policy that requires mandatory reporting of cybersecurity incidents? | ✗ | As of August 2014, there is no legislation or formal requirement for mandatory cybersecurity incident reporting in Croatia. |
| 11. | Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)? | ✗ | There is no legislation or policy in place in Croatia 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 Croatia, as of August 2014. |
| | **OPERATIONAL ENTITIES** | | |
| 1. | Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)? | ✓ | National CERT <www.cert.hr> was established in 2009. It is responsible for coordinating security and incident response measures for parties that use a Croatian IP address or .hr domain.<br>ZSIS CERT <www.zsis.hr>, the CERT of the Information Systems Security Bureau, has jurisdiction over the Croatian government institutions. |
| 2. | What year was the computer emergency response team (CERT) established? | 2009 | |
| 3. | Is there a national competent authority for network and information security (NIS)? | ✓ | The Information Systems Security Bureau (ZSIS) <www.zsis.hr> is the national competent authority for network and information security for Croatia, as stated in the Act on Information Security 2007 <www.soa.hr/UserFiles/File/information_security.pdf>. It operates under the Office for National Security.<br>The Croatian Regulatory Authority for Network Industries (HAKOM) <www.hakom.hr> is an independent entity with public authority as prescribed by the Electronic Communications Act 2008. HAKOM engages in part with cybersecurity in carrying out its duties. |
| 4. | Is there an incident reporting platform for collecting cybersecurity incident data? | ✓ | National CERT <www.cert.hr> is tasked with managing the reporting of cybersecurity incidents. National CERT provides an online reporting structure to log cybersecurity incidents. |
| 5. | Are national cybersecurity exercises conducted? | ◑ | Croatia has participated in cybersecurity exercises conducted by both the European Union and NATO. |
| 6. | Is there a national incident management structure (NIMS) for responding to cybersecurity incidents? | ✗ | ZSIS CERT <www.zsis.hr> is tasked with the incident response and management of government institutions exclusively. It does not, however, operate within an established national incident management structure. |
| | **PUBLIC-PRIVATE PARTNERSHIPS** | | |
| 1. | Is there a defined public-private partnership for cybersecurity? | ◑ | There is no defined public-private partnership for cybersecurity in Croatia.<br>The National CERT <www.cert.hr> has jurisdiction over all parties that use a Croatian IP address and will liaise with private organisations for the purpose of cybersecurity incident prevention and incident response.<br>The Croatian Regulatory Authority for Network Industries (HAKOM) <www.hakom.hr>, itself an independently-run public authority, liaises with the private sector in its support role of the communication industry.<br>RACVIAC — Centre for Security Cooperation <www.racviac.org> is a representative body for the defence and security sectors in southeastern Europe, based in Croatia. |
| 2. | Is industry organised (i.e. business or industry cybersecurity councils)? | ✗ | There is no significant industry-led platform for cybersecurity in Croatia. |
| 3. | Are new public-private partnerships in planning or underway (if so, which focus area)? | ✗ | There are no new public-private partnerships being planned in Croatia. |

## COUNTRY: CROATIA

| | QUESTION | RESPONSE | EXPLANATORY TEXT |
|---|---|---|---|
| | **SECTOR-SPECIFIC CYBERSECURITY PLANS** | | |
| 1. | Is there a joint public-private sector plan that addresses cybersecurity? | ◑ | There is no public-private sector plan that addresses cybersecurity.<br>However with a specific body, the Croatian Regulatory Authority for Network Industries (HAKOM) <www.hakom.hr> is a public authority that supports the communication industry. HAKOM liaises with the private sector in the course of its duties. |
| 2. | Have sector-specific security priorities been defined? | ✖ | Sector-specific security priorities have not been defined. |
| 3. | Have any sector-specific cybersecurity risk assessments been conducted? | ✖ | Sector-specific risk assessments have not been released, as of August 2014. |
| | **EDUCATION** | | |
| 1. | Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age? | ✖ | Croatia participates in the Balkan Security Agenda, which promotes cybersecurity education in the region, but a specific Croatian education strategy or program has not yet been developed. The Balkan Security Agenda Cyber Defence and Cybersecurity Initiative <www.balsec.org/category/blog/bsa-cyber-defence-and-cybersecurity-initiative> includes a recommendation to "increase public awareness of how individuals can protect their own internet data, and promote cyber-security education and training". |