DCAF Geneva Centre for Security Sector Governance

Developing a cybersecurity crisis management plan

Tadas Jakštas

May 2023

About DCAF

DCAF – Geneva Centre for Security Sector Governance is dedicated to improving the security of states and their people within a framework of democratic governance, the rule of law, respect for human rights, and gender equality. Since its founding in 2000, DCAF has contributed to making peace and development more sustainable by assisting partner states, and international actors supporting these states, to improve the governance of their security sector through inclusive and participatory reforms. It creates innovative knowledge products, promotes norms and good practices, provides legal and policy advice and supports capacity-building of both state and non-state security sector stakeholders. DCAF's Foundation Council members represent over 50 countries and the Canton of Geneva. Active in over 70 countries, DCAF is internationally recognized as one of the world's leading centres of excellence for security sector governance (SSG) and security sector reform (SSR). DCAF is guided by the principles of neutrality, impartiality, local ownership, inclusive participation, and gender equality. For more information visit www.dcaf.ch and follow us on Twitter @DCAF_Geneva.

DCAF – Geneva Centre for Security Sector Governance
Maison de la Paix
Chemin Eugène-Rigot 2E
CH-1202 Geneva, Switzerland
Tel: +41 22 730 94 00
info@dcaf.ch
www.dcaf.ch
Twitter @DCAF_Geneva
Design & layout: DTP studio
Author : Dr. Tadas Jakštas
ISBN : 978-92-9222-710-4

Developing a Cybersecurity Crisis Management Plan

On 21-22 October 2022, DCAF – the Geneva Centre for Security Sector Governance, brought together legal experts from the Western Balkans for a Seminar on National Cybersecurity Legislation in Veles, North Macedonia. The seminar was organised in close cooperation with the Ministry of Information Society and Administration of the Republic of North Macedonia, as part of DCAF's three-year regional project, 'Good Governance in Cybersecurity in the Western Balkans', funded by the United Kingdom's Government's Foreign and Commonwealth Office (FCDO). During the event, the participants and experts discussed approaches to cyber crisis management and the importance of a cybersecurity crisis management plan. This report summarizes key insights shared and provides information on developing a cybersecurity crisis management plan.

Introduction

The growing reliance on technologies offers many advantages which have improved our economy and quality of life. However, it also makes us more vulnerable to those who attack our digital infrastructure to undermine our national security, economic prosperity, and public safety. Cyber incidents are becoming more and more frequent, and this trend is unlikely to be reversed soon. The most significant of these incidents can result in demonstrable harm to the national security interests, foreign relations, or economy of the country or to its public health and safety.

Since the availability, integrity, confidentiality and resilience of critical infrastructures and response to cyber threats have emerged as national priorities for all developed nations, deliberate planning, coordination, and exercising of response activities is necessary in order to minimize the threat and consequences to the nation.

The development of a comprehensive cyber crisis management plan is the prerequisite of crisis management.

What is a National Cyber Crisis Management Plan?

It is an organisational measure and can be defined as follows:

- A strategic framework which articulates the roles and responsibilities, capabilities and coordinating structures that support how a nation responds to and recovers from significant cyber incidents that pose risks to critical infrastructure.
- A strategic plan which recommends and elaborates on the actions and responsibilities for a coordinated and multidisciplinary approach that responds to and recovers from nationally significant cyber security incidents.

Purpose for developing a National Cyber Crisis Management Plan

- Establish roles and responsibilities of the stakeholders during a crisis situation
- Devise ways to resolve incidents
- Ensure proper information sharing among stakeholders
- Serve as a basis for improving the management and coordination of cyber incidents at the institutional level
- Set the effective communication channel for message passing related to the incident
- Below is an example of a formulated objective[1]:

1 Republic of Lithuania National Cyber Incident Management Plan, approved by decree No. 1209 of the Government of the Republic of Lithuania of 5 December 2018

> "[The objective of] the National Cyber Incident Management Plan is to set out] procedures for cyber incident management while defining cyber incident categories, cyber incident information, cyber incident investigation and cyber incident analysis after cyber incident investigation is over." (National Cyber Incident Management Plan of the Republic of Lithuania)

Elements of a National Cyber Crisis Management Plan

A National Cyber Crisis Management Plan should provide a formal, focused, and coordinated approach to responding to incidents that provides the roadmap for implementing the incident response capability at the national level. The plan shall lay down the following elements:

Objectives of national preparedness measures and activities:

The National Cyber Crisis Management Plan should lay out objectives of national preparedness measures and activities:

- To recommend and elaborate on the actions and responsibilities for a coordinated and multidisciplinary approach that responds to respond and recovers from cyber security incidents of national significance impacting critical systems and the economy.
- To minimize disruption of services or loss/theft of information caused by incidents.
- To use the information gained for better preparation or future handling of incidents.

Tasks and responsibilities of the national competent authorities:

The National Cyber Crisis Management Plan should clearly describe tasks and responsibilities required to be performed by each assigned authority during cyber crisis management at strategic, operational and technical levels. The examples of tasks and responsibilities could include, among others:

Strategic level

- Identify the impacts of the disruptions caused by the crisis on the functioning of the country.
- Activate additional crisis management mechanisms depending on the nature and impact of the incident. These may include, for example, a Civil Protection Mechanism.
- Take diplomatic measures to respond to the national cyber crisis.
- Make available emergency support, for example by additional cyber response powers that could include the use of cyber reserve forces, if applicable.
- Cooperate and coordinate with international organisations and partner countries.
- Assess national security and defence implications.
- Decide upon a common communication strategy towards the public.

Operational level

- Preparing decision-making at the strategic level by providing, for example, situational awareness reports.
- Coordinate the management of the cybersecurity crisis, as appropriate, by involving other incident response stakeholders in the country, including CII operators, sectoral CERTs, agencies responsible for cybercrime, and national defence.
- Alert entities impacted by the information security incident or those that can contribute to the response and provide those entities with the required information to understand their role and any expectations that might exist regarding their cooperation and support.
- Assess the consequences and impact at the national level and propose possible remediation actions.

Technical level

- Incident handling during a cybersecurity crisis.
- Monitoring and surveillance of an incident, including continuous analysis of threats and risk.

During a cyber crisis, the timely engagement of the appropriate level of governance bodies will focus both management and operations to prevent, detect, respond to and recover from the crisis. It is therefore important that the National Cyber Crisis Management Plan includes the governance structure that will ensure the implementation of the cyber crisis roles and responsibilities. Several examples of bodies[2] involved at strategic, operational and technical level could include:

Strategic level bodies

- Cybersecurity Committee
- Executive Management Team
- National Cybersecurity Committee
- Cybersecurity Council
- Cybersecurity Advisory Council

Operational level bodies:

- National CERT
- National Cyber Security Agency
- Sectoral CERTs
- Other incident response agencies responsible for cybercrime, national defence, etc.

Technical level bodies

- Critical Information Infrastructure operators
- Private sector organisations
- Vendors

Below are examples of formulated tasks and responsibilities of the national competent authorities in the Australian Government Crisis Management Framework[3]:

> "[The] National Cyber Security Committee (NCSC) – is the mechanism for inter jurisdictional coordination for technical responses to cyber security incidents.
> The NCSC members include the Head of the Australian Signals Directorate's Australian Cyber Security Centre (HACSC), the cyber security state and territory lead from each jurisdiction and supporting representatives from PM&C and the Department of Home Affairs.
> - The NCSC escalates the Cyber Incident Management Arrangements (CIMA) and classifies the cyber security alert level by severity, which dictates the technical response activities and coordination undertaken to remediate the cyber security incidents and mitigate the threat to other Australian entities."

Crisis management procedures and information exchange channels:

The goal of the development of crisis management procedures is to codify the methods and protocols to facilitate information sharing and cyber crisis coordination to support operational-level cooperation and preparedness, detection and analysis, containment, eradication, and recovery and post-incident activity.

2 Please note that the titles of respective governance bodies depend on concrete national context.

3 Commonwealth of Australia, Department of the Prime Minister and Cabinet, Australian Government Crisis Management Framework, Australian Government Crisis Management Framework, Version 3.2 November 2022

Examples of cyber crisis management procedures that could be elaborated in the National Cyber Crisis Management Plan include:

Information distribution to relevant stakeholders: As the response to a crisis progresses, information must be distributed and disseminated. The procedure should describe what kind of information, when and by what means the information needs to be distributed to relevant stakeholders.

Information security status reporting: The procedure involves delivering concise and factual information about the current status of cybersecurity inside the constituency. As a crisis might be used to start other attacks, or as occurring attacks might be part of the overall activities leading this crisis, it is important for the crisis management team to establish complete situational awareness.

Strategic decisions communication: The procedure involves informing all other relevant stakeholders in a timely manner about the impact of the crisis.

Initiation of cross border cooperation: The national emergency management authority (national CERT) should be able to initiate cross-border cooperation with CERTs and national competent authorities to mitigate the consequences and effects in cyber space.

When it comes to information exchange, the following channels could be used during the crisis:

- **Email:** participants may exchange information up to the level TLP:GREEN via unencrypted emails. For any information above that level, secure communication is required.
- **Phone:** phone could be used to call Point of Contacts or the Functional Phones of respective agencies.
- **Conference call:** a conference call could be organised using secure equipment and nationally adopted platforms, e.g., MS Teams, Webex, Zoom, etc.
- **Portal:** stakeholders may exchange files in a secure manner using the Customer Portal.
- **MISP:** stakeholders may exchange indicators of Compromise through the MISP.

Preparedness measures, including exercises and training activities:

In addition to the crisis response phase, the National Cyber Crisis Management Plan should include crisis preparedness measures. Preparedness is defined by ongoing training, evaluating and corrective action, ensuring the highest level of readiness, as well as pre-crisis declaration. The preparedness measures could include:

- Developing capacity building activities in the field of operational cybersecurity, including respective technologies (e.g., CTI, Cyber Ranges) and implementing additional responses and cyber crisis management;
- Organising and participating in national cybersecurity exercises for testing crisis management procedures. The staff appointed to execute specific roles and responsibilities should undertake relevant internal and external training and exercise opportunities. It is recommended to clarify which trainings and exercises are strongly recommended and which are optional for the staff involved.
- Organising communication checks to test, at a procedural level, the readiness of participants to communicate efficiently and exchange information as well as their response time. Communication checks may be scheduled on a regular basis and always prior to the cyber exercises above, in order to address proactively any problems.
- Sharing and implementing lessons learnt from previous incidents, crises and exercises.

Relevant public and private interested parties and infrastructure involved:

Cybersecurity is a collective effort, and it is important to identify relevant public and private interested parties and infrastructure to be involved. The preparedness, response and recovery phases of cyber crises are influenced by a range of elements and played out by various stakeholders. Examples include government bodies, critical infrastructure operators and private bodies. Roles should be clarified and outlined, in terms of how they will collaborate to manage expectations throughout the process and achieve success.

Examples of stakeholders:

Internal:

- Law enforcement
- Private sector
- Critical sectors
- Vendors

External:

- Foreign law enforcement agencies
- CERTs

National procedures among relevant national authorities and bodies

The National Cyber Security Crisis Management Plan should entail relevant procedures in relation to three core objectives: situational awareness, coordinated response and public communications. Example of procedures that could be defined in the National Cyber Security Crisis Management Plan include:

- Monitoring and drafting ad-hoc reports on ongoing, large-scale incidents and crises;
- Setting up and coordinating the activities of relevant national cybersecurity stakeholders in cyber crises;
- Identifying the impacts of disruptions caused by the crisis on the functioning of the country;
- Exchanging mitigation and response strategies and measures based on situational awareness (complementing technical incident response), through national cyber crisis response mechanisms;
- Activating technical mitigation measures and coordinating technical capacities needed to stop or reduce the impact of the attacks on the targeted information systems;
- Cooperating with relevant third parties (international partners, private sector, etc.);
- Taking diplomatic measures to respond to the cyber crisis;
- Activating additional crisis management mechanisms/instruments, depending on the nature and impact of the incident. These may include, for example, the Civil Protection Mechanism and cyber reserve forces.
- Contributing towards common public messages regarding the incident or crisis;
- Sharing lines to take (LTT) and communication strategies.

Conclusion

A National Cyber Crisis Management Plan can be prepared effectively by the deliberate inclusion of several key elements. It must have a clear set of objectives, and an articulation about the tasks and responsibilities from strategic, operational and technical levels (engaging relevant bodies for each one). It should also outline the processes and protocols for information exchange and responses during a crisis, and indicate key aspects of preparedness and training so that all stakeholders know the specifics of their functions. National procedures can ensure effectiveness and completements of situational awareness, coordinated response and public communications. Overall, what is most critical is clarity upfront about the actors involved, how they relate with one another, and what each does before and during a crisis, in order to mitigate its effects.

References and Further Reading

Cyber Incident Response Plan Guidance
https://www.cyber.gov.au/sites/default/files/2022-07/ACSC%20Cyber%20Incident%20Response%20Plan%20Guidance_A4.pdf

Computer Security Incident Response Team (CSIRT) Services Framework Version 2.1.0
https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0_bugfix1.pdf

National Cyber Concept for Crisis Preparedness and Management
https://www.gov.il/BlobFolder/news/cybercrisispreparedness/en/Management%20of%20crisis%20situations%20english%20final.pdf

National Cyber Incident Management Plan of the Republic of Lithuania
Available in Lithuanian from: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr#part_5a4a17b82cc64cf4ba1dc41021eada4d

National Cyber Incident Response Plan
https://www.cisa.gov/uscert/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

TRAFFIC LIGHT PROTOCOL (TLP), FIRST Standards Definitions and Usage Guidance — Version 2.0
https://www.first.org/tlp/

DCAF Geneva Centre for Security Sector Governance

P.O.Box 1360
CH-1211 Geneva 1
Switzerland

info@dcaf.ch
+41 (0) 22 730 94 00

www.dcaf.ch

@DCAF_Geneva