Factsheet 5: Cyber Crisis Communication & Enhancement of Organizational Resilience

Cyber crisis communication refers to the strategic management of information during and after a cybersecurity incident. It involves timely, accurate, and transparent communication with stakeholders to mitigate the impact of the incident on an organisation's reputation, operations, and stakeholders' trust with the use of actionable information. By focusing on enhancing organisational cyber resilience, DYNAMO s also working on improving cyber crisis communication. DYNAMO's main interest in the crisis communication aspect of the project is on supporting the improvement of cyber resilience across the entire resilience lifecycle (see Factsheet 3 for further information about resilience) through a coherent risk and crisis communication strategy.

Importance of Cyber Crisis Communication

Effective crisis communication is essential for managing and mitigating the impact of crises on critical infrastructure. It ensures the timely dissemination of information, helps to coordinate response measures, and maintains public confidence. In the event of a cyberattack, time is of crucial importance. A timely response can help contain the spread of the attack and limit its impact on critical systems, data and operations. By initiating communication activities and notifying relevant stakeholders and organisations as soon as possible we can mobilise resources and implement remediation measures more effectively. Transparent communication can help organisations maintain control over the reporting of cyber incidents. Effective communication during a cyber crisis can help prevent the situation from escalating further. By promptly informing internal teams, external partners and regulators of the nature and severity of the incident, organisations can coordinate their risk mitigation efforts and prevent secondary attacks or additional vulnerabilities from being exploited. By providing accurate information about the nature and scope of the breach, as well as the steps being taken to remediate it, companies can curb the spread of misinformation that can exacerbate the crisis. Clear communication can also reassure stakeholders, including customers, employees, investors, and the public, that the organisation is actively managing the situation and working towards a resolution.

Enhancing Organizational Resilience with Cyber Crisis Communication across the Resilience Lifecycle

Cyber crisis communication is intricately linked to maintaining organisational resilience throughout the resilience lifecycle by facilitating effective communication before, during, and after cyber incidents. Here is how cyber crisis communication contributes to maintaining organisational resilience at each stage of the resilience lifecycle:

1. **Preparation:**
   Communication Planning: As part of preparation, organisations develop communication plans that outline strategies, protocols, and procedures for communicating during cyber crises. These plans identify key stakeholders, communication channels, messaging frameworks, and escalation procedures to ensure a coordinated and effective response.
2. **Prevention:**
   Educating Stakeholders: Effective cyber crisis communication includes educating stakeholders about cybersecurity best practices and preventive measures to reduce the likelihood of cyber incidents. By raising awareness and promoting a culture of cyber security, organisations can proactively mitigate cyber risks and vulnerabilities.
3. **Detection:**
   Alerting Stakeholders: When a cyber incident is detected, timely communication is critical to alert stakeholders about the situation and initiate response efforts. Clear and transparent communication helps ensure that relevant parties are aware of the incident and can take appropriate actions to mitigate its impact.
4. **Response:**
   Coordination and Collaboration: During a cyber crisis, communication plays a central role in coordinating response efforts and collaborating with internal teams, external partners, and regulatory authorities. By maintaining open lines of communication, organisations can share information, allocate resources, and make timely decisions to contain and mitigate the incident.
5. **Recovery:**
   Providing Updates: Throughout the recovery process, organisations communicate with stakeholders to provide updates on remediation efforts, restoration of services, and measures taken to prevent future incidents. Transparent communication helps rebuild trust and confidence among stakeholders and demonstrates the organization's commitment to addressing the aftermath of the crisis.
6. **Adoption:**
   Learning and Improvement: Post-crisis communication includes conducting a thorough review of the incident response process, analysing lessons learned, and identifying areas for improvement. By communicating insights and recommendations for enhancing cyber resilience, organisations can drive continuous improvement and adaptation to future cyber threats.

In essence, cyber crisis communication is integral to maintaining organisational resilience by facilitating effective communication strategies and practices at every stage of the resilience lifecycle. By prioritizing transparent, timely, and coordinated communication, organizations can enhance their ability to prevent, detect, respond to, recover from, and adapt to cyber incidents, ultimately strengthening their overall resilience to cyber threats.

Funded by the European Union under grant agreement no. 101069601. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.