INFORMATIONAL

ACSC and CISA Release Business Continuity in a Box

TLP:WHITE

Nov 13, 2023

On November 13, 2023, the Australian Signals Directorate’s Australian Cyber Security Centre (ACSC) and the Cybersecurity and Infrastructure Security Agency (CISA) released communications to bolster organizations' resiliency and stand up critical business functions during or following a cyber incident.

The dissemination, Business Continuity in a Box, helps organizations maintain or re-establish the basic functions needed to operate a business while responding to the issues impacting critical systems.

Reference(s)	CISA, Australian Government

Release Date
Nov 14, 2023 (UTC)

Alert ID 8236da51

View Alert

Tags business continuity, ACSC, CISA

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

ENISA
ENISA works with organisations and businesses to strengthen trust in the digital economy, boost the resilience of the EU's infrastructure, and, ultimately, keep EU citizens digitally safe.

It does this by sharing knowledge, developing staff and structures, and raising awareness.

For additional information, please review publications, including the Procurement Guidelines for Cybersecurity in Hospitals and the CSIRT Capabilities in Healthcare Sector.

HICP
The Health Industry Cybersecurity Practices (HICP) refer to a set of guidelines and recommendations developed by the U.S. Department of Health and Human Services (HHS) to help healthcare organizations improve their cybersecurity posture. The HICP was created in response to the increasing threat of cyberattacks and data breaches in the healthcare sector, which has been a target for cybercriminals due to the sensitive and valuable nature of healthcare data.

The HICP resources are aimed at helping healthcare organizations of all sizes, including small, medium, and large entities. It provides practical and actionable guidance for managing and mitigating cybersecurity risks in healthcare environments, with a focus on five key cybersecurity threats: ransomware, phishing, loss or theft of equipment or data, insider threats, and attacks against connected medical devices.

For Questions or Comments
Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**