NIST

Cybersecurity Framework Success Story

Israeli National Cyber Directorate

The voluntary Framework for Improving Critical Infrastructure Cybersecurity was developed through a collaborative process by industry, academia, and government stakeholders. It enables organizations – regardless of size, sector, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improve security and resilience. NIST does not validate or endorse any individual organization or its approach to using the Cybersecurity Framework.

CYBER DEFENSE METHODOLOGY FOR AN ORGANIZATION

Ver. 2.0

> “The ‘NIST Cybersecurity Framework’ has served as a solid and beneficial basis for developing the Israeli "Cyber Defense Methodology for the Organization". Furthermore, harmonizing our methodology with leading standards creates an internati onal cyber defense language which supports collaboration against global cyber threats.”
>
> -Igal Unna, Director General,
> Israel National Cyber Directorate (INCD)

Organizational Profile

- Like many other nations, the Israeli economy consists of small and medium-sized businesses, corporations and other enterprises, including many that are key to its success. The Israeli economy relies heavily on information technology (IT) and operational technology (OT), hence many businesses are vulnerable to different types of cyber risks.
- The cybersecurity of Israel’s critical information infrastructure (CII) has been guided, but not extensively regulated, by the state since 2002. Some sectors have implemented varying levels of regulation, yet most of the market is not regulated for cybersecurity risk management.
- In 2012, the Prime Minister's Office established the Cyber Bureau responsible for promoting cybersecurity in Israel, known today as the Israeli National Cyber Directorate (INCD). Its responsibilities include promoting the resilience of the Israeli market against cyber threats.
- In 2017, INCD published the Israeli Cyber Defense Methodology (ICDM) 1.0, which adopts the NIST Cybersecurity Framework 1.0 – making it available for implementation by the Israeli Market.
- In 2021, INCD published the next generation of the methodology, ICDM 2.0 which adopts the NIST Cybersecurity Framework 1.1, NIST SP 800-53 Rev. 5 and additional NIST standards. In addition, the new methodology adopts MITRE Threat-Information Defense and Zero-Trust paradigms.

Situation

- Stakeholders recognized the need for an easily-adopted approach for achieving cybersecurity objectives and better protecting important resources.
- Legacy methodologies focused on "Identify, Protect and Recover" outcomes; the application of the NIST Cybersecurity Framework is seen as strengthening "Detect and Respond" considerations. In addition, the adoption of the up-to-date NIST Cybersecurity Framework, NIST SP 800-53 Rev. 5, NIST SP 800-160 series and other relevant NIST standards, improve the ICDM security defense controls.
- Developing an international common language is of utmost importance for Cyber Defense. The Cybersecurity Framework was seen as enabling Israeli stakeholders
(such as industry, academia and government) to engage with international colleagues.
Stakeholders needed a flexible framework that could map local and international standards as well as reduce the workload required to demonstrate compliance.

PRIME MINISTER’S OFFICE
NATIONAL CYBER DIRECTORATE
NATIONAL CYBER SECURITY AUTHORITY

NIST National Institute of Standards and Technology
U.S. Department of Commerce

Situation (Continued)

- INCD intended to build upon previous experience from CII and local regulations, in addition to other international models such as ISO 27001 and the NIST Risk Management Framework.
  Many organizations work with global security software and products, that help present the organization's compatibility with NIST's methodology. Adhering to this framework helps the market to adopt the Israeli methodology more smoothly and quickly.
- INCD chose NIST Cybersecurity Framework as the basis for building the methodology for the Israeli economy.

Process

- ICDM is multilayered to improve user experience and to ease implementation. Each control contains layers of information including the requirement, organizational maturity model, explanations and examples, links to best implementation practices, example templates, relevance to confidentiality/ integrity/availability, selected standards and regulations compatibility.
- The development process of the ICDM included Proof of Concept adoption by various government offices, both maturing the methodology and providing the office with a structured work plan for 2021. In 2021, the whole Israeli government adopted ICDM as the required cyber risk methodology for its offices.
- INCD is in active dialog with selected regulators to adopt the ICDM for implementation in their sectors. Training of professionals on the Israeli methodology is simpler, since it is based on the NIST Cybersecurity Framework - which is familiar to the relevant academics and relevant professionals. This has helped to more easily assimilate Israeli methodology in the training and implementation phase.
- INCD has conducted many awareness activities to explain "Why" and "How" to use the ICDM. These include outreach for CISOs and another designed for other C-levels; conferences for CISOs, legal advisors, consulting firms, and risk managers; training for Israel National Cyber Event Readiness Team (CERT-IL) to provide hotline assistance to the market; and translation of the ICDM to English to aid Israeli companies' international cooperation.

Combined Benefits/Results

- The methodology synchronizes the common international cybersecurity language of the Cybersecurity Framework among the various Israeli stakeholders
  (economy, academia, government).
- By choosing the NIST Framework, it was simpler to convince regulatory and legal professionals to support the methodology, since they knew it was well-established, tested, and implemented in many organizations around the world.
- ICDM provides a flexible framework to meet various sectoral and market needs.
- Since the ICDM was published in June 2021, it has been adopted voluntarily by many organizations in the Israeli market.

What's Next

- Increase efforts to expand accessibility and assimilation of ICDM in the economy.
- Automate the ICDM 2.0 process in a free application, available on the INCD website.
- Incorporate ICDM 2.0 as the basis for guidance in various sectoral regulators' work plans in 2022.
- Establish a national ICDM-based certification scheme for secure organizations. Work to harmonize an ICDM certification scheme with leading international standards.
- Using OSCAL: The Open Security Controls Assessment Language to automate the ICDM 2.0 deployment process and validation.

Contact Information & Resources

Israel National Cyber Directorate (INCD) Website:
https://www.gov.il/en/departments/general/cyber_security_methodology_2
INCD contact: Yuval Sinay (yuvalsin@cyber.gov.il)

Develop ICDM 2.0 to include CII and new updates.
Cyber Defense Doctrine 2.0
https://www.gov.il/en/departments/general/cyber_security_methodology_2