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.

Organizational Profile

- The Israeli economy is comprised of small and medium-sized businesses, corporations, and other enterprises, including many that are key to its information infrastructure. Like most other nations, the Israeli economy relies heavily on information technology (IT) and operational technology (OT), which leaves the nation and its businesses vulnerable to many 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 government 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), which adopts the NIST Cybersecurity Framework – making it available to be implemented by the whole economy of Israel.

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.

CYBER DEFENSE METHODOLOGY FOR AN ORGANIZATION

VER. 1.0

> "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 international cyber defense language which supports collaboration against global cyber threats."
>
> -Igal Unna, Director General,
> Israel National Cyber Directorate (INCD)

Situation (Continued)

- Developing an international common language is of utmost importance for Cyber Defense. The Cybersecurity Framework was seen as enabling Israeli stakeholders (industry, academia and government) to engage with international colleagues.
- Stakeholders needed a flexible framework that could map to local and international standards as well as reduce the workload to achieve and record adherence to multiple regulations.
- INCD wanted 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, which helps present the organization's compatibility with NIST's methodology. Adhering to this Framework helps the economy 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. Most of the controls that allow the method to be implemented are also derived from NIST (Special Publication 800-53).

Process

- ICDM is multilayered to improve ease of use. Each control contains layers of information including the requirement, explanations and examples, links to best implementation practices, example templates, relevance to confidentiality/integrity/availability, selected standards and regulations compatibility.
- ICDM development included Proof of Concept adoption by various government offices, both maturing the methodology and providing the office with a structured work plan for 2018. In 2018, 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. The Environment Protection sector adopted the ICDM and incorporated it into the Hazardous Materials Act, requiring every company handling hazardous materials to apply the ICDM. A similar process is being established with health, finance and other regulated sectors. In fact, all of these help to implement the Framework language in the economy.
- Training of professionals for 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.

RECOVER
IDENTIFY
CYBERSECURITY FRAMEWORK
RESPOND
PROTECT
DETECT

Combined Benefits/Results

- 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 method, since they knew it was well-established, tested, and implemented in many organizations around the world.
- Provides a flexible framework to meet various sectoral and market needs.
- Since the ICDM was published in June 2017, 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 process in a free application, available on the INCD website. The first module, addressing supply chain, has been released along with updates to the full ICDM module. Embedding the array app into organizations' compatibility with the NIST Framework, including Framework-based reports and graph development.
- Incorporate ICDM as the basis for guidance in various sectoral regulators' work plans in 2019.
- Establish a national ICDM-based certification scheme for secure organizations. Work to harmonize an ICDM certification scheme with leading international standards.
- Develop a new organizational maturity model in 2019 based on ICDM.
- Develop ICDM 2.0 to include CII and new updates.

Contact Information & Resources

- Israel National Cyber Directorate (INCD) Website:
  https://www.gov.il/he/departments/policies/cyber_security_methodology_for_organizations
  INCD contact: Yuval Segev (yuvals@cyber.gov.il)
- NIST Cybersecurity Framework Website:
  https://www.nist.gov/cyberframework
  NIST contact: cyberframework@nist.gov