Israel leads 10-country simulation of major cyberattack on world markets

10-day drill led by Finance Ministry aims to boost international cooperation against hacker threat to global financial systems

By **TOI STAFF**
9 December 2021, 11:02 pm

An illustrative image of computer popup box screen warning of a system being hacked; hackers, cybersecurity attack. (solarseven; iStock by Getty Images)

Israel led a 10-country, 10-day-long simulation of a major cyberattack on the world's financial system by "sophisticated" players, with the goal of minimizing the damage to banks and financial markets, the Finance Ministry said on Thursday.

The Finance Ministry led the scenario with help from the Foreign Ministry, and said the "war game" was the first of its kind.

The exercise simulated several scenarios, including sensitive data surfacing on the dark web alongside fake news, leading to global financial chaos.

Participants included representatives from the US, UK, United Arab Emirates, Germany, Italy, Austria, Switzerland, the Netherlands, Thailand, the International Monetary Fund and the World Bank.

The Finance Ministry's chief economist, Shira Greenberg, headed the Israeli team. The exercise was "further evidence of Israel's global leadership" in the field of financial cyber defense, she said.

"The unique and groundbreaking exercise held today showed the importance of coordinated global action by governments together with central banks in the face of financial cyber threats," Greenberg said.

The simulation "featured several types of attacks that impacted global foreign exchange and bond markets, liquidity, integrity of data and transactions between importers and exporters," Reuters reported.

Israeli officials said international cooperation was the only way to counter the threat of major cyberattacks.

"Attackers are 10 steps ahead of the defender," said Micha Weis, financial cyber manager at the Finance Ministry.

In October, the National Cyber Directorate issued a general warning to Israeli businesses to be aware of potential cyberattacks, as the country faced an uptick in hacking attempts.

Prime Minister Naftali Bennett speaks at the annual Cyber Week, at Tel Aviv University, on July 21, 2021. (Miriam Alster/FLASH90)

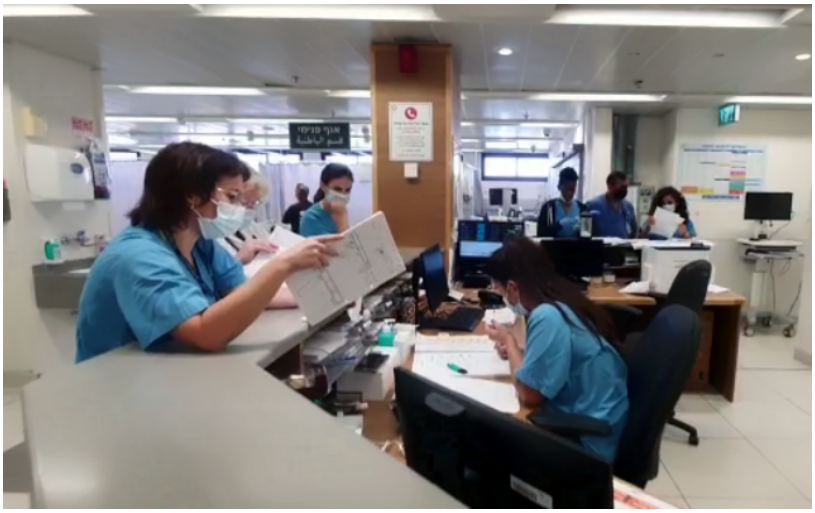
The warning came after an Israeli hospital faced a major ransomware cyberattack that crippled systems, and from which it could take several months to recover.

On Wednesday, Israel's National Insurance Institute said that its website had been hacked, causing it to go offline for several hours.

In July, cybersecurity firm Check Point reported that Israeli institutions are targeted by about twice as many cyberattacks as is average in other countries around the world, particularly the country's health sector, which experiences an average of 1,443 attacks a week.

The most targeted sectors around the world, including in Israel, are education and research, followed by government and security organizations, and then health institutions, Check Point said.

The report found that, on average, one in every 60 Israeli organizations or firms is targeted every week with ransomware attacks, an increase of 30 percent over the rate in 2020.



Hospital staff at Hillel Yaffe Medical Center log patient details with pen and paper, following a ransomware cyberattack, October 13, 2021. (Hillel Yaffe Medical Center)

Last month, the Black Shadow hacking group released what it said was the full database of personal user information from the Atraf website, an Israeli LGBTQ dating service and nightlife index.

The group also uploaded personal medical information for patients of Israel's Machon Mor medical institute, including medical records of some 290,000 patients.

The two attacks amounted to one of Israel's largest-ever privacy breaches.

Black Shadow is a group of Iran-linked hackers who use cyberattacks for criminal ends, according to Hebrew media reports.