G7 boost banking cybersecurity as new SWIFT threat emerges

WASHINGTON, USA: The G7 group of leading economies laid out a new framework for battling the hacking of financial institutions on Tuesday, 11 October 2016, as a new threat using the SWIFT interbank network emerged.

© Gleb Shabashnyi – 123RF.com

Reacting to a rise in hacking incidents that have robbed banks of everything from client databases to hundreds of millions of dollars, the G7 group issued a set of principles for banks to implement cybersecurity programs.

"The recent incident involving the SWIFT network and other cyberattacks really underscore the imperative for robust cyber security throughout the global financial sector," said US Treasury Deputy Secretary Sarah Bloom Raskin.

"These threats have not destabilized the financial sector but they threaten to destabilize it," she said.

Raskin is co-chair of the Cyber Expert Group of the G7 - the United States, Canada, France, Germany, Italy, Japan, and the United Kingdom.

The two-page "Fundamental Elements of Cybersecurity" outlines the building blocks of an effective risk-based bank program to defend itself and the broader financial system from cyber threats.

The guidelines are aimed at public and private sector financial institution board members and top management to use for shaping and assessing their company's cyber strategy.

The stunning theft earlier this year of $81 million from Bangladesh's central bank drew attention to the vulnerabilities of financial sector institutions to cyber threats, especially those using the SWIFT worldwide network for interbank transfers.

After the Bangladesh heist, SWIFT said the incident was "not a single occurrence, but part of a wider and highly adaptive campaign targeting banks."

That has elevated the alarm levels in the world's leading finance ministers and central bank chiefs.

"The challenge with cyber security is that the threat vectors can be difficult to discern and are constantly morphing in search of financial sector vulnerabilities," said Raskin.

That issue was underscored Tuesday when computer security group Symantec issued a warning over a new malware threat to financial organisations called "Odinaff".

Odinaff has been deployed widely around the world since January 2016 in attacks that "appear to be extremely focused on organisations operating in the banking, securities, trading, and payroll sectors," it said.

Symantec said the Odinaff attackers make use of some of the infrastructure used by some earlier attacks tapping the SWIFT network known as Carbanak. Yet another group, known as Lazarus, is believed behind the Bangladesh threat.

"These attacks require a large amount of hands on involvement" with "a heavy investment in the coordination, development, deployment, and operation" of the tools used to break into the targets' systems, Symantec said.

Source: AFP