Follow Us

Sanction Implications for US Financial Institutions

Summary

As the US, UK, Canada, and European Union continue to apply pressure against Russian entities and oligarchs through economic sanctions US institutions, should anticipate immediate and future retaliation that can direct attacks against financial institutions and indirect attacks affecting critical infrastructure, resulting in supply chain disruption. FS-ISAC has seen three "malware wipers" used against Ukraine, and our members have also reported Zoom and frozen asset freezing themed phishing emails targeting US banking executives.

The global cyber threat level was raised to ELEVATED following the start of the conflict. This level means there is a heightened level of cyber risk. As the situation changes rapidly, the Cybersecurity Infrastructure and Security Agency (CISA) have guided organizations to raise their defensive shields and remain vigilant.

During a recent FS-ISAC Spotlight Call regarding cyber-preparedness against the backdrop of the Russo-Ukraine (RU/UKR) conflict, attendees said "there is a significant degree of uncertainty by financial institutions on whether they are indeed prepared to handle a Russian cyber-attack. This is possibly due to the gap between expectations and reality so far in terms of the cyber-attack landscape." Jake Williams, a former National Security Agency hacker, told Joseph Menn and Craig Timberg of the Washington Post recently, "*If an attacking army is going to use cyberattacks, the most useful moment is probably at the beginning of the operation when it can do the most to undermine, confuse and demoralize the adversary*". Therefore, overall cyber hygiene is the best protection.

Is your institution…

- *Providing regular updates about the geopolitical situation to senior executive teams?*
- *Taking steps now to harden your networks in preparation for a potential cyber-attack?*
- *Validating that your third-party, supply-chain vendors and managed security service providers (outsourced providers) are meeting your information security standards?*
- *Sharing information with your peers to help everyone adapt and protect quickly?*
- *Monitoring changes to the economic sanction landscape to remain OFAC compliant?*

For internal discussion…

- *Where is your institution obtaining threat intelligence?*
- *Have you identified 'triggers' that can indicate that your organization is being probed for weaknesses?*
- *Have you adjusted your security controls and processes due to the elevated risk in response to the RU/UKR situation?*
- *Have you reviewed and recently tested your incident response plans in the event of a cyber-attack?*

Learn more about…

- ⓘ *Shields Up Guidance for Organizations*
- ⓘ *Five Cybersecurity Actions for Executives*
- ⓘ *Four Things You Can Do to Keep Yourself Cyber-Safe*

Contact information

All organizations should report incidents and anomalous activity to CISA 24/7 Operations Center at central@cisa.dhs.gov or (888) 282-0870 and/or to the FBI via your local FBI field office or the FBI's 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov. FS-ISAC members should report cyber incidents to IncidentReporting@fsisac.com or within the *Share* portal.

Events

Three-Day US Spring Summit
27—30 March 2022

Cyber-Range Exercises
Ransomware
13 April 2022
26 April 2022

More info: fsisac.com/events

About FS-ISAC

Contact

Jeffrey Korte

Director, Community Institution and Associations Council

Reach out to Jeffrey on LinkedIn

☎ 703.962.7901 ext. 583