IN THIS ISSUE: The Invasion of Ukraine, MFG-ISAC

The Invasion and its Impact

GRF's Business Resilience Council is committed to its mission of keeping members informed of systemic, geopolitical, and business risk; on Feb 24, before dawn, Russia launched a multi-pronged invasion into Ukraine. Multiple military targets have been attacked and civilians are attempting to leave cities in large numbers, many headed to Poland, as Russian forces prepare to lay siege. Ukraine said it has experienced several cyberattacks against its government and financial sectors, including DDoS and a wiper attack.

This invasion was preceded by months of Russian troop buildup along Ukraine's borders -covered in past BRC meetings- including in Russian-allied Belarus and near Ukraine's eastern Donbass region, an area with two Russian-affiliated separatist centers. The Russian government officially recognized the two areas, Donetsk and Luhansk, as independent republics on February 21, paving the way for Russian military forces to enter the area. A much larger invasion of Ukraine has since commenced, with assaults against major cities like Kyiv and Kharkiv.

The reason Russian President Putin gave for the invasion was to demilitarize and "denazify" Ukraine and to protect ethnic Russians from genocide. Claims of genocide have been widely regarded as false, and Russia has engaged in multiple disinformation campaigns featuring alleged violence against innocents.

In response to the invasion, the EU, US and other NATO members agreed to remove Russia from the SWIFT international payment network, sanctioned major banks and Russian officials, prevented Russia from accessing international accounts, stopped development of the Nord Stream 2 pipeline, blocked technology exports, sent weaponry for Ukraine's defense, and closed off airspace to all Russian planes, including private jets.

Putin has promised a severe response to any nation that impedes his invasion and has made repeated references to being a nuclear-armed power, putting some nuclear forces on alert. So far, the Russian military has not captured the capital of Kyiv, bogged down by what analysts say was stronger than predicted resistance by the Ukrainian military and militias. There have also been reports of Russian logistical challenges in keeping its forces fed, armed and fueled.

On February 28, Ukraine officially applied to become a member of the EU. Ukrainian President Zelensky asked for expedited approval but it is not certain if all EU member states will agree. Meanwhile, delegations from Russia and Ukraine met in Belarus to negotiate an end to the conflict but no agreement has yet been concluded.

The US has committed to defending its NATO allies near Ukraine and will deploy more troops to Germany.

Invasion Cont...
NATO has also enabled its high readiness forces to deploy to protect allies in eastern Europe. The NATO secretary general added that a cyberattack against a NATO member could trigger an Article 5 response in which all NATO members consider the act an attack.

US President Biden stated that if Russia uses cyberattacks against the US or its critical infrastructure, the US is prepared to respond. Overall, analysts say that US and Europe should be prepared for cyberattacks as sanctions and lethal aid are provided to Ukraine, or as "spillage" occurs during cyberattacks against Ukrainian or Ukrainian affiliated organizations.

On February 21 The US Cybersecurity & Infrastructure Security Agency (CISA) released "Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure." Organizations are also encouraged to review CISA's Shields Up resources.

From a supply chain perspective, the invasion may have broad, lasting effects. Russia and Ukraine together account for nearly 30% of the world's wheat. Ukraine also ships machinery, chemicals, and raw minerals while Russia is a major exporter of oil and natural gas. Amid sanctions, consumers and governments will see rising prices at the pumps; both Shell and BP announced they would divest from Russian projects. Analysts also predict additional shortages and higher prices for hydrocarbon minerals and metals, which will in turn affect manufacturing across the globe.

New Manufacturing ISAC
GRF, in partnership with The Cybersecurity Manufacturing Innovation Institute (CyManII), has launched the Manufacturing Information Sharing and Analysis Center (MFG-ISAC), a nonprofit cybersecurity threat awareness and mitigation community for small, medium and enterprise-level manufacturers in the United States. Visit www.mfgisac.org for more information or follow @MFG_ISAC on Twitter or Manufacturing ISAC on LinkedIn.

GRF Ransomware Report
GRF analysts just completed a year-end update of the semi-annual ransomware report tracking attacks based on public sources and conversations of threat actors in closed forums. Analysts compiled data on 1,200+ incidents in the second half of 2021.

Some key findings:
-The predominance of Conti gave way to LockBit RaaS from the first half of the year to the second
-Analysts observed the emergence of small-scale and politically motivated ransomware operations
-Critical Manufacturing, Financial Services, and Retail (Commercial Facilities Sector) continue to be the top targeted sectors
-GRF analysts believe the IT sector will overtake the Financial Services sector as the most heavily targeted industry, primarily driven by supply chain and third-party service attacks

COMMUNITY CONTACTS
OT-ISAC (John Lee)
LS-ISAO (Raquel Santiago)
EASE (Tim Chase)
ProSIX (Mark Orsi)
K12 SIX (Doug Levin)
BRC (Chris Denning)
MFG-ISAC (Tim Chase)

Cross-Sector Call, Events & Community Updates

Cross-Sector Call
Impressions from a first-time joiner: "There was a tangible collegiality to the call. Threats and recent attacks were discussed, with the conversation bouncing around the attendees. The feel was informal, yet the information was there. Impressive sharing of ideas and answers to questions coming from nearly all attendees. With the free exchange of ideas, it was interesting to see how many of the speakers knew each other. The call was impressive, with sharing of ideas and answers to questions. Anyone who is eligible to join the calls should consider participating."

Business Resilience Council Events
The BRC, an all source, multi sector community for business and operational resilience, held a TLP White briefing with Mandiant on "Hardening your business environment against destructive Russian cyber activity." The BRC also held a members-only webinar the following week on implications and impacts to businesses stemming from the invasion. Nearly 350 people attended from more than a dozen sectors. The panelists, from Europe and the US, outlined steps their organizations are taking to shore up their defenses and how they're addressing the new challenges of operating in Europe and Asia.
The next BRC event will be on March 30 covering extremism and domestic terrorism in the US.

K12 SIX Events
On February 17, K12 SIX hosted a webinar on why and how to implement its baseline cybersecurity standards for school districts. View the archived presentation. On March 10, join K12 SIX for the Second Annual K12 Cybersecurity Leadership Symposium

OT-ISAC Summit Call for Presentations
The OT-ISAC Annual Summit will be a hybrid event on September 7-8, 2022, with OT and IT experts sharing best practices and lessons learned for the mutual defense of critical assets.

OT-ISAC CISO Roundtable
The March 17 roundtable will strengthen collaboration between critical asset owners, operators and government, to advance collective defense efforts. The event is open to c-level security leaders that are not members of OT-ISAC.

Key points of discussion:
- The changing OT threat landscape and threat scenarios in Asia-Pacific
-How ransomware attacks impact OT environments
-Operational resilience and supply chain risk.
-Why collaboration and information sharing are key to achieving cyber resilience

GRF Summit Registration and Call for Presentations
GRF has opened early bird registration and its call for presentation for the 2022 Summit on Security & Third-Party Risk. The in person event will be October 27-28 at the Gaylord National Resort outside Washington, DC. Sessions will focus on third-party and supply chain security issues, vendor management, cybersecurity, intelligence sharing, geopolitical threat mitigation, and emerging compliance and regulation.