

IN THIS ISSUE: VIRAL OPERATIONS & THE THREAT TO UKRAINE

Pandemic Impacts

During a Business Resilience Council (BRC) [webinar](#) on the future of business operations, Paul Benda, Senior Vice President of Operational Risk and Cybersecurity at the American Bankers Association, provided insights on how the pandemic has affected the financial sector.

Benda explained that at the beginning of the pandemic some banks were moving to suspend drive-through operations. However, they saw an uptick in use as an alternative to in-branch services as the pandemic continued. But the question of operational cadence remains; many sectors are facing serious challenges maintaining staff. Paul cited the “Great Resignation” and wage inflation as continuing challenges, in conjunction with COVID-19.

Courtney Romolt, Programs Director for Healthcare Ready, also joined the webinar to provide a healthcare perspective on Omicron’s impact to operations. She described demand surges for COVID-related protective products, workforce issues and changing information and policies as challenges for the sector.

Distributors are dealing with personal demand for products, as well as commercial-level needs. Throughout the pandemic, misinformation and disinformation from malicious actors have proven to be a problem for caregivers as well.

Rapid interpretation and incomplete data have muddled messaging to the public and presented challenges for treatment and personal protective equipment (PPE) guidance.

Looking beyond the sector, more than 3 billion people have not had their first dose of vaccine. Focus now needs to be given to vaccination, to prevent a more virulent variant.

Ukraine

The unfolding threat of invasion in Ukraine and subsequent impacts to Europe and the world were covered by Chris Denning, Chief Security Officer at GRF. What does Putin want? He likely seeks broader geopolitical influence in Europe, strengthened domestic control by offering an external threat, and a return to Russian hegemony in the region, diminished in the ‘90s. Putin is putting pressure on Ukraine, NATO, and the rest of Europe to see what he can achieve.

How likely is an invasion? Denning outlined how Putin will almost certainly seek to achieve the most for the least cost. As of the BRC webinar, Russia issued several extreme demands to the United States and NATO to which they responded “no,” but offered to continue dialogue.

Staci Elliott, Geopolitical and Physical Security Analyst for GRF, pointed out that most of the possible consequences for Russia focus on sanctions, including sanctions against Putin himself.

Ukraine Cont.

Those sanctions may not be a deterrent as Putin's face-value concern is the presence of NATO near Russia's perceived sphere of influence. Of note, Ukraine has experienced WhisperGate malware attacks. Cyber-attacks were also utilized prior to the Russian invasions of the Crimea region and the country of Georgia.

COVID-19

Moving to COVID-19, Elliott highlighted declining case numbers in the US, UK and South Africa, but warned that reported numbers are not always current due to global data collection methods. Schools are also returning to meeting in classrooms rather than online, and more children are getting vaccinated. But there is the threat of new variants on the horizon, with the report of a new sub-variant recently announced.

Webinar topics were in line with the BRC mission to provide info on physical and systemic risk including geopolitical crisis, severe weather events, pandemic news, and other potential threats to commercial operations. For more info, contact [Chris Denning](#) or to join, [click here](#).

BRC Products and Services:

- Weekly Threat and Resilience Report
- Situation Reports for Sustained Emergencies
- Quantified Threat Calculation
- Cross-Sector Emergency Operations Dashboard
- Secure Sharing Portal
- Scheduled All Sector, All Source Threat Calls
- Sector Specific Resilience Discussions
- Regulatory Guidance Meetings and Reports

Community Updates & Events

Oil & Natural Gas ISAC

In January ONG-ISAC focused on automation efforts and an incentive challenge for members. Staff is now completing the cross-sector Semi-Annual Ransomware Report. For more information contact [Hassan Shahzad](#).

K12 SIX

-National Director Doug Levin presented at the US DHS School Safety Task Force and the Dept. of Education's Office of Educational Technology co-hosted event on building resilience in the K12 sector.

-With the support of the Bill & Melinda Gates Foundation, K12 SIX was invited by the State Ed. Tech. Directors Association to partner on awareness and resources for managing cyber risk.

-A K12 SIX community document on Log4j vulnerability in 90+ products:

<https://www.k12six.org/news/k12-six-releases-k12-specific-log4j-collaboration-resource>

-February 11: K12 SIX Workshop "Kickstart Your Cybersecurity Plan in 2022"

-March 10: Second Annual K12 Cybersecurity Leadership Symposium

LS-ISAO

At the outset of Log4j, members, analysts and vendor partners came together to share warning and mitigation activities. Kudos to everyone who not only balanced their primary workload but took the time to share what they learned with others. LS-ISAO would also like to recognize two security vendors for their help; reps from iManage and Intapp went above and beyond.

CONTACTS

OT-ISAC ([John Lee](#))

LS-ISAO ([Raquel Santiago](#))

EASE ([Tim Chase](#))

ProSIX ([Mark Orsi](#))

K12 SIX ([Doug Levin](#))

BRC ([Chris Denning](#))