Conflict in the Ukraine: Business and Risk Management Implications

Overview

The coordinated attack by Russia on Ukraine has created a historic risk environment for operations in these countries, and for organizations around the world. Companies with interests in Russia, Ukraine and nearby eastern European countries, as well as multinational organizations, should be aware that the current situation is fluid and evolving. There could be potential for negative impacts to clients' businesses due to:

- Political violence/nationalization.
- Trade interruption, including supply chain disruption/destruction.
- Increased cyberattacks.
- The ability to enter or leave the region safely.
- Possible expropriation of Western assets in Russia.

In This Update

There will also be an increase in energy and commodity prices in Europe and possibly globally, depending on conflict escalation. Organizations within the conflict region and across the globe can expect an increase in terrorism, supply chain disruptions and cyberattacks, and should take necessary steps to protect their operations.

We have created this report to help clients identify potential emergent threats to their businesses and to assist by highlighting the following overall risk management considerations:

1. Work to ensure the security of your company's people, assets, and supply chains, including:
    a. Establish a risk map or risk summary of operations and locations in conflict zone — include property values and employee counts as critical data.

Continued on next page

b. Identify the need for and establish critical alternative/redundant supply chains.

c. Determine alternative geographic locations for rapid recovery.

d. Log, update and provide best practices to traveling employees.

2. Review and maintain hard/physical copies of all insurance policies, critical contacts, claim reporting detail and disaster recovery and business continuity plans to allow quick access in the event of a cyberattack.

3. Submit any notice of circumstance or claim to your insurance companies as soon as possible following consultation with internal/external risk management.

4. Engage all current cyber risk management protocols and address critical vulnerabilities discovered. Conduct deep dive into cyber "hygiene" to seek to mitigate potential as a target and increase employee threat awareness training.

5. Finally, understand the ongoing business risks in the conflict region will be critical. These may include global impacts around financial transfer difficulties (due to SWIFT sanctions), commodity pricing impacts, cargo and aviation risks due to lack of insurance available and heightened risk of sanction violations.

Below are additional details to help organizations prepare for the business and risk management implications of the Ukraine crisis. For more information or resources, please contact your USI representative.

Considerations for Property and Casualty

Property Supply Chain and Business Interruption Losses

Business interruption (BI) coverage is a component of many property policies, and seeks to indemnify a policyholder, in case of a covered loss, for the income that would have been earned had no loss occurred, subject to limitations in the coverage forms. Coverage is written on an "actual loss sustained" basis and is often factored as net income plus continuing expenses. BI coverage responds to losses during a period of suspended operations as the result of property damage.

Most (if not all) policies require a "direct physical loss or damage of the type insured herein" at an insured location to trigger business interruption coverage. This is considered as a "direct exposure."

Business income losses from direct exposures are fairly straightforward, however, we would anticipate a majority of losses from the conflict in Ukraine to be "indirect" in nature (i.e., business shut down related to supply chain disruptions, as opposed to actual physical damage), and likely not covered by a standard BI policy.

For indirect exposures, examine any policy extensions for potential coverage, including:

- Contingent time element, including variations such as dependent property and supply chain.
- Civil/military authority.
- Ingress/egress.

These coverage extensions typically have the same trigger as direct BI: "direct physical loss or damage of the type insured herein." For the coverage extensions, the property damage occurs away from an insured premise. It is important to note that these coverage extensions have specific limitations that need to be reviewed on a per policy basis. It is critical to review the policy against loss details to understand the potential of specific limitations (e.g., war exclusions, territorial limitations, time/geographic qualifiers, percentage deductibles, waiting periods, aggregates, sub-limits, etc.) and how they may apply to sustained losses.

Policy coverage, terms and conditions vary — contact your USI representative with questions or for assistance.

Continued on next page

Potential Challenges With Property Claims

- Difficulty and delay in investigations.
- Difficulty and delay in verifying actual damages.
- Coverage issues arising out of damages caused by war; carefully review your policy for language and definitions related to war.
- Difficulty and delay in providing proof of loss to the insurance company.
- A general delay in claim payments will most likely result.

Claims Review and Filing

Some considerations for filing a claim:

1. Review your claims management plans.
2. Refer to the USI claim reporting manual for proper reporting of your loss. Obtain a claim number and any contact information available at the time of reporting.
3. Document your losses (as possible) and continue to do so.
4. Take steps to mitigate losses or to protect property from additional damage, but only when it has been confirmed to be safe to do so.
5. Appoint a person as the primary point of contact regarding the business interruption claim who can serve as a liaison between the various operations and claims personnel. Set up an internal cost code to track costs/losses.
6. In the event of employee injuries or fatalities, document employee name, a complete description of loss, date of loss, and situation leading up to the loss (i.e., any external factors that may have contributed).

Considerations for Cyber Risk

Experts agree that Russian-backed or supported cyberattacks and counterattacks intended to disrupt supply chains, IT suppliers, governmental agencies, financial services organizations, critical infrastructure (including healthcare, transportation, and energy) and other critical national institutions are already happening and will likely continue.

Cyber Risk Management Protocols

All organizations, regardless of the location of their operations, should seek to improve their cyber hygiene and take a holistic view of cyber risk management. Recent underwriter focus suggests the following control areas may be linked to increased likelihood of ransomware incident or susceptibility to cyberattack. Areas to review include:

- Employee training and awareness of suspicious phishing communications (from email but also text message, social media and voicemail), particularly in regard to targeted "spear phishing" related to the conflict in Ukraine.
- Multifactor authentication (MFA).
- Endpoint detection and response (EDR) and/or extended detection and response (XDR).
- 24/7 network monitoring and security operations center (SOC).
- Encrypted, secure network backups.
- Network segmentation, particularly for "end of life" (EOL) systems, and cadence for pathing vulnerabilities.

Additional Resources

For additional information, visit the U.S. Cybersecurity and Infrastructure Security Agency (CISA) website at www.cisa.gov/shields-up, or Information Sharing and Analysis Centers (ISAC), as applicable, www.nationalisacs.org.

Continued on next page

- Incident response plans.
- Vendor and supply chain risk management (third-party risk management) — especially critical as attacks spread widely.

Contact your USI representative with questions or for assistance addressing cyber risks.

Challenges With Cyber Insurance: Cyber Risk and War

Policy language may affect how claims are covered, if at all. Review your policy for several key definitions and exclusions:

- Cyber war definitions/exclusions, including:
  - Causation wording for war exclusions.
  - Potential cyber terrorism carve-backs. Carve-backs are typically limited to cyberattacks conducted by individuals or groups with particular ideological goals, not conducted on behalf of a nation state (e.g., Russia, North Korea, etc.).
  - Cyber terrorism extensions or exclusions.
- The scope of sanction and Office of Foreign Assets Control (OFAC) exclusions.
- The scope of computer network/operations.

Cyber Claims Reporting

Cyber incidents/events or claims should typically be reported as soon as possible after discovering (or reasonably suspecting) such incident or becoming aware of such claim.

Importantly, insureds are typically required to use insurance-company-approved counsel and vendors as the overall breach coach/incident response vendors for activities including, but not limited to, forensics, public relations, data restoration, valuations, regulatory notification, etc. Each carrier has pre-approved vendors and breach coaches. This process is intended to maintain privilege as well. "Standard" claim reporting is also required — breach coach use is not considered "reporting."

Other lines of coverage may also be impacted by a cyber event. Proper reporting should be made after consultation with stakeholders and a review of insurance policy portfolio. This may include notice to property, general liability, crime, kidnap and ransom, directors and officers liability, and others. USI can help with determining process, procedure and discuss potential reporting implications.

In addition to the areas noted above, USI's comprehensive cyber risk control continuum includes services and solutions designed to assess current cyber hygiene and exposures to cyber risk, and to connect clients and prospects with curated third-party providers that specialize in addressing emergent cyber risks. Our solutions, such as Answerlytics™ and a customized eRiskHub can assist clients in improving cybersecurity and insurance marketability, pricing and terms.

How USI Can Help

As the situation continues to evolve and sanctions potentially elevate, experts expect to see an increase in global cyberattacks and counterattacks, as well as significant and likely sudden disruptions to the global supply chain. We will continue to closely monitor the situation and advise clients.

Please contact your local USI representative to review the details of your risk and any losses or ongoing exposures to risk against specific policies and risk management procedure, or visit us at www.usi.com.