Cyber considerations from the Russia-Ukraine war

Remain proactive in your cyber security preparedness

March 2022

kpmg.com

After months and weeks of tension, the Russian government's invasion of Ukraine has elevated concerns for cyber security incidents and the resilience of critical business functions. Beyond protecting their employees and supporting the people of Ukraine, international businesses are also assessing their exposure and vulnerability to cyber incidents, technology disruption, and related impacts and resilience of critical services. These threats may arise from nation-backed attacks on systems and infrastructure or may be the direct results of armed conflict. While there is significant uncertainty around the Russia-Ukraine war and associated actions, including their duration, the lasting nature of their impacts, or their reach, there are some things we all should consider as we evaluate our level of cyber security preparedness.

Resilience and continuity

Whether there are localized business operations in one of these nations, neighboring countries, or only in the West, businesses should assess their readiness for cyber incidents and ability to recover from a cyber-attack. Reviews of response plans should be conducted to understand exposures to current threat scenarios that may have increased in likelihood due to business profile, geography, or perceived affinities.

Steps to take

— Review the threat landscape for your business and collect related intelligence

— Understand incident response and resilience planning, asking 'how often you have tested your plans' and 'how relevant the testing scenarios are to current threats

— Refresh security incident response plans, and have a specific ransomware incident response plan that is tied to an overall security incident response plan

— Identify a short list of critical dependencies that may be impacted by current events and conduct an analysis of risks, likelihood of incident, and preparedness, making prioritized plans for remediation

— Consider running a table-top exercise if one has not been performed in the last six months

Partner and vendor risks

At the beginning of the pandemic, as businesses were shut down and our employees, partners, and customers were sent home, we realized very quickly how interdependent we all had become. Businesses had become far more reliant on ecosystems of third parties providing critical systems, services, and data, as well as people to support enabling processes and technologies. While the current situation is different, it highlights once again the importance of understanding the security and resilience of all partners across the critical areas of our supply chains.

What to do

— Identify the dependencies on vendors and partners from Ukraine, Russia, and neighboring countries and build a contingency plan should they be cut off from the supply chain

— For the critical suppliers (at a minimum), have an increased monitoring of network traffic from that part of the world, as cybercrime is expected to get more sophisticated with many hacking groups having a free hand in the current situation

— For the critical suppliers (at a minimum), understand the incident response and resilience planning they have put in place

— Understand the cascading effect to the organization of an incident in your supply chain and determine the weak links to focus on, through increased monitoring and being response ready

Cyber security monitoring and incident response

It is widely expected that there will be a marked increase in activity against Ukrainian targets, their allies, and supporters. The Russian government has made strong statements against business entities attempting to exit the country and it could be expected that there will be a related increase in cyber-attacks against them as well. Businesses should be on heightened alert especially those that are considered part of critical infrastructure, including Oil, Energy, and Financial Services firms, as they are often priority targets in time of war.

What to do

— Understand the cyber security monitoring capabilities across your network infrastructure to make sure that strong incident detection and prevention capabilities are in place and have adequate coverage of your business, systems, and data

- Work with cyber security intelligence partners to better understand the risk for your business and actions to take, and consider attending daily threat briefings in the near term
- Consider engaging with cyber security vendors for managed detection and response services to help augment your own capabilities, or to provide skilled support to a critical need
- If you have a cyber threat hunt team, have them look for specific indicators of compromise (IOCs) based on known Russian bad actor tactics, techniques, and procedures (TTPs)
- Make sure that you have a cyber security incident response firm on retainer, and that contracts are up to date
- Review any required cyber security incident regulatory reporting requirements for your business
- Consider proactive discussions with law enforcement and government agencies that would be involved in the event of a major cyber security incident

Workforce support

To alleviate resourcing challenges, we have found that organizations are considering or have already added surge support capabilities to manage business-as-usual security functions, triaging an increased volume of security alerts, and/or execution of project portfolios. Some businesses who have operations in impacted regions have also looked for temporary support to cover critical services until their employees can return to office or country.

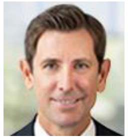
What to look for

- Extended staff shortages
- Regions impacted by current events

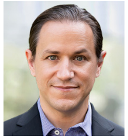
Summary

The Russia-Ukraine war is driving increased concerns for cyber security incidents and the resilience of critical business functions and services. While the current climate is unpredictable, there are things we can do to better understand our readiness, capabilities, and requirements to help reduce the impacts and shorten the durations of incidents when they occur.

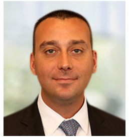
Contact us



Kyle Kappel
Principal
Cyber Security Services
Network Leader
E: kylekappel@kpmg.com



Rik Parker
Principal
Cyber Security Services
E: rikparker@kpmg.com



Charlie Jacco
Principal
Cyber Security Services
E: cjacco@kpmg.com

Jonathan Dambrot
Principal
Cyber Security Services
E: jdambrot@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.