Cyber considerations from the conflict in Ukraine

How to stay on top of your cyber security preparedness

KPMG International

home.kpmg

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, amongst international organizations. Beyond protecting their employees and supporting the people of Ukraine, international businesses are also assessing their exposure and vulnerability of their critical services to cyber incidents, technology disruption and supply chain impacts. These threats may arise from nation-backed attacks on systems and infrastructure, the direct result of armed conflict or collateral damage from that conflict. While there remains a significant amount of uncertainty around the conflict, including the duration, scale and reach, there are some key considerations that can help to evaluate cyber security preparedness levels.

Threat

There has been a marked increase in cyber threats against Ukrainian targets, which is widely expected to extend to their allies and supporters.[1]

The Russian government has made strong statements regarding actions it would take against business entities attempting to exit the country including nationalization of assets.[2]

Organizations should be prepared for a potential increase in cyber-attacks in retaliation to such exits. In addition, as they are often considered to be priority targets in times of conflict, those business considered part of the critical infrastructure, including energy, telecommunications, media and financial services firms should also be on heightened alert.

Whether there are localized business operations in Russia, Ukraine, neighboring countries, or only in the West, businesses should assess their readiness for cyber incidents and their ability to recover from a cyber-attack as part of broader preparedness.

Resilience and incident preparedness

Reviews of existing response plans should be conducted to better understand exposures to current threat scenarios that may have increased likelihood due to business profile, geography or perceived affinities.

What you can do

— Review the threat landscape for your business, work with cyber security intelligence allies to better understand the business risk and actions to take, and consider attending daily threat briefings in the near term.

— Plan for disruption of operations in the impacted region and how to minimize risk to the business if those operations are compromised, which may include disconnection of functions or additional security controls.

— Review incident response and resilience plans asking: How often you have tested your plans? How relevant the testing scenarios are to current threats?

— Refresh security incident response plans and have a specific ransomware response plan that supports the overall plan.

— Review your cyber insurance policies and coverage, including any exemptions which may apply.

— 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.

— Consider proactive discussions with law enforcement and government agencies that would be involved in the event of a major cyber security incident.

— Consider running a table-top exercise simulating an organization's response to a cyber-attack if one has not been performed in the last 6 months.

Cyber security protection

Given the heightened concerns over cyber threats, it makes sense to review a key set of cyber security controls which may help reduce the likelihood of a successful attack, particularly those which help defend against state or organized crime threats which may arise from the conflict.

What you can do

— Prioritize the patching of any critical system vulnerabilities which are being actively exploited. The US Cybersecurity and Infrastructure Security Agency (CISA) maintains a database of these vulnerabilities, and many national cyber security centers offer advice on areas to prioritize.

[1] Alert: Destructive Malware Targeting Organizations in Ukraine, CISA, March 01, 2022.
[2] Mauro Orru, "Russian Commission Backs Nationalization of Exited Western Businesses," The Wall Street Journal, March 9, 2022.

— Review access controls to key systems focusing on the use of multi-factor authentication, removal of unused or expired accounts, and the necessary isolation of high-risk systems.

— Ensure anti-malware software is installed, licenses are up to date and software is regularly updated.

— Carry out external vulnerability scans for internet-facing systems, and address any major issues found.

— Confirm backup processes are in place for critical systems, and regular offline copies of vital business data are taken.

Cyber security monitoring

While pragmatic improvements can be made to cyber security protective measures, effective security monitoring is vital to help timely detection and response to any intrusion. The average time between initial compromise and triggering of destructive malware is now measured in days rather than weeks or months.

What you can 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.

— If you have a cyber threat hunt team, have them look for specific indicators of compromise (IOCs) based on tactics, techniques and procedures (TTPs) linked to state or organized crime groups involved in the current conflict.

— Consider engaging with cyber security vendors for managed detection and response services to help augment your capabilities or to provide skilled support to a critical need.

People

This is a time of concern and uncertainty for many people. Businesses should plan for disruption of their operations in the impacted region, in some cases having to arrange for temporary support to cover critical services until their employees can return to the office or country.

As well as supporting employees and their families, organizations should also be aware of the risks of organized crime groups. These groups look to exploit the current crisis by establishing fake websites purporting to offer support and information or by seeking donations. There will also likely be Ukraine-themed phishing campaigns and potential targeting of high-profile individuals based on their expressed views over this crisis.

What you can do

— Ensure employees have access to authoritative sources of information on the current crisis and are made aware of the risk of phishing and fake websites themed around the crisis.

— Offer cyber security advice to employees in high-risk locations or roles.

— Consider surge support to manage business-as-usual security functions, triage the increased volume of security alerts, and undertake urgent security improvements.

Partner, vendor and supply chain risks

At the beginning of the COVID-19 pandemic, as businesses shut down and employees, partners and customers were sent home, organizations quickly realized how interdependent they all had become on a complex ecosystem of third parties providing critical systems, services and data. Once again, the conflict in Ukraine highlights the importance of understanding the security and resilience of all partners across the vital areas of your supply chains.

What you can 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 critical suppliers (at a minimum) have increased monitoring of network traffic from countries involved in the conflict, 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 impact on your organization of potential incidents in your supply chain to determine where to focus increased monitoring and greater readiness to respond.

Next Steps

The conflict in Ukraine is driving increased concerns for cyber security incidents and the resilience of critical business functions and services. While the current climate is unpredictable, consider how the situation may develop and the scenarios that may arise. For each scenario, explore what this means for your organization in terms of people, business, supply chains and technology risks — with cyber security as one element of that broader view.

In the meantime, some considerations can be actioned now to prepare for those eventualities, improve resilience, reduce the impact and shorten the duration of incidents if and when they occur.

Contacts

Akhilesh Tuteja
Partner,
KPMG in India
Global Cyber Security Leader
E: atuteja@kpmg.com

Dani Michaux
Partner,
KPMG in Ireland
EMA Cyber Security Leader
E: dani.michaux@kpmg.ie

Matthew O'Keefe
Partner,
KPMG Australia
Asia Pacific Cyber Security Leader
E: mokeefe@kpmg.com.au

Ravi Sankar
Principal,
KPMG in Caricom
KPMG Islands Group Cyber Security Leader
E: RSankar@Kpmg.Com.jm

home.kpmg/socialmedia

Designed by Evalueserve.

Publication name: Cyber considerations from the conflict in Ukraine
Publication number: 137993-G
Publication date: March 2022