Ukraine conflict: Cyber considerations

KPMG Board Leadership Centre

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 Ukraine conflict and associated actions, including their duration, the lasting nature of their impacts, or their reach, there are some things all boards should consider as they look to management to evaluate their cyber security preparedness.

Resilience and continuity

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 threats. Ensure management:

- Review the threat landscape and collect related intelligence
- Understand incident response and resilience planning, asking how often the plans have been tested 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 prioritised plans for remediation
- Consider running a table-top exercise if one has not been performed in the last six months

Partner and vendor risks

Businesses have become far more reliant on third parties providing critical systems, services, data, and support. It is vital to understand the security and resilience of all partners across critical areas. Ensure management:

- Identify the dependencies on vendors and partners from Ukraine, Russia, and neighbouring countries and build a contingency plan should they be cut off from the supply chain
- Monitor network traffic as cybercrime is expected to get more sophisticated with many hacking groups having a free hand in the current situation
- Understand the incident response and resilience planning in place for the critical suppliers (at a minimum)
- Understand the cascading effect of an incident in the supply chain and have determined 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. Businesses should be on heightened alert for these attacks, especially those considered part of critical infrastructure, including Oil, Energy, and Financial Services firms, as they are often priority targets in time of war. Ensure management:

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

— Work with cyber security intelligence partners to better understand the risk to the business and the actions to take, and consider daily threat briefings in the near term

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

— Seek indicators of compromise based on known bad actor tactics, techniques, and procedures.

— Secure a cyber security incident response firm and make sure the 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.

Workforce support

To alleviate resourcing challenges, consider adding surge support capabilities to manage business-as-usual security functions, triage the increased volume of security alerts, and/or execute project portfolios.

Businesses that have operations in impacted regions might also look for temporary support to cover critical services until their employees can return to work. Ensure management are considering:

— Extended staff shortages.

— Regions impacted by current events.

The Ukraine conflict 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.

The KPMG Board Leadership Centre

The KPMG Board Leadership Centre offers support and guidance to non-executive directors, whether managing a portfolio non-executive career or embarking on a first appointment. Membership offers you a place within a community of board-level peers with access to topical and relevant seminars, invaluable resources and thought leadership, as well as lively and engaging networking opportunities. We equip you with the tools you need to be highly effective in your role, enabling you to focus on the issues that really matter to you and your business.

Learn more at www.kpmg.com/uk/blc.

Contact us

Timothy Copnell
Board Leadership Centre
T: +44 (0)7801 520802
E: tim.copnell@kpmg.co.uk

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 on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2022 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.
CREATE. | CRT141495A