Cybersecurity + geopolitical conflict: What boards and CEOs should know and do

February 2022

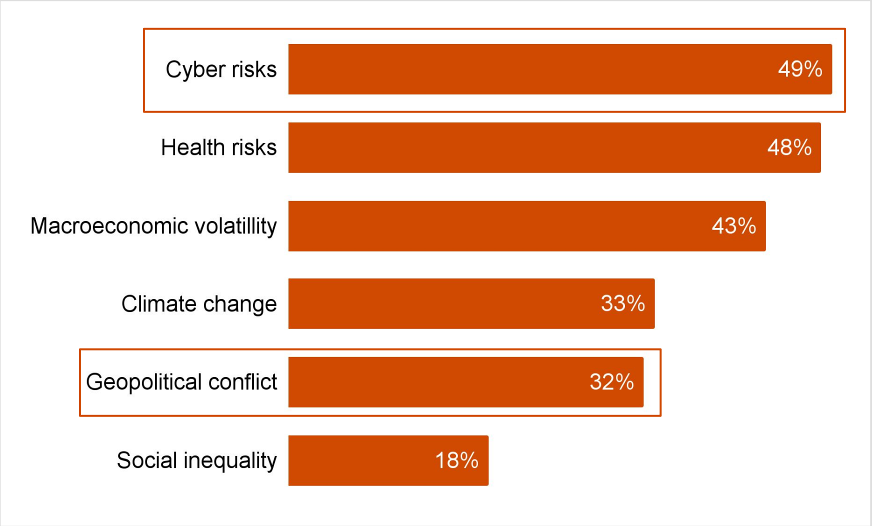
pwc

Cyber + geopolitical conflict – What boards and CEOs should know and do

Cybersecurity and geopolitical conflicts. Separately, they are among the top worries of CEOs, according to PwC's CEO Survey. Together, the combined risks pose an even bigger challenge that demands immediate action.

CEOs and boards should be asking: Are we ready to mitigate escalating cyber risks related to geopolitical tensions that might flare up in 2022?

Elevated risk environment for business when cyber risks and geopolitical conflicts combine

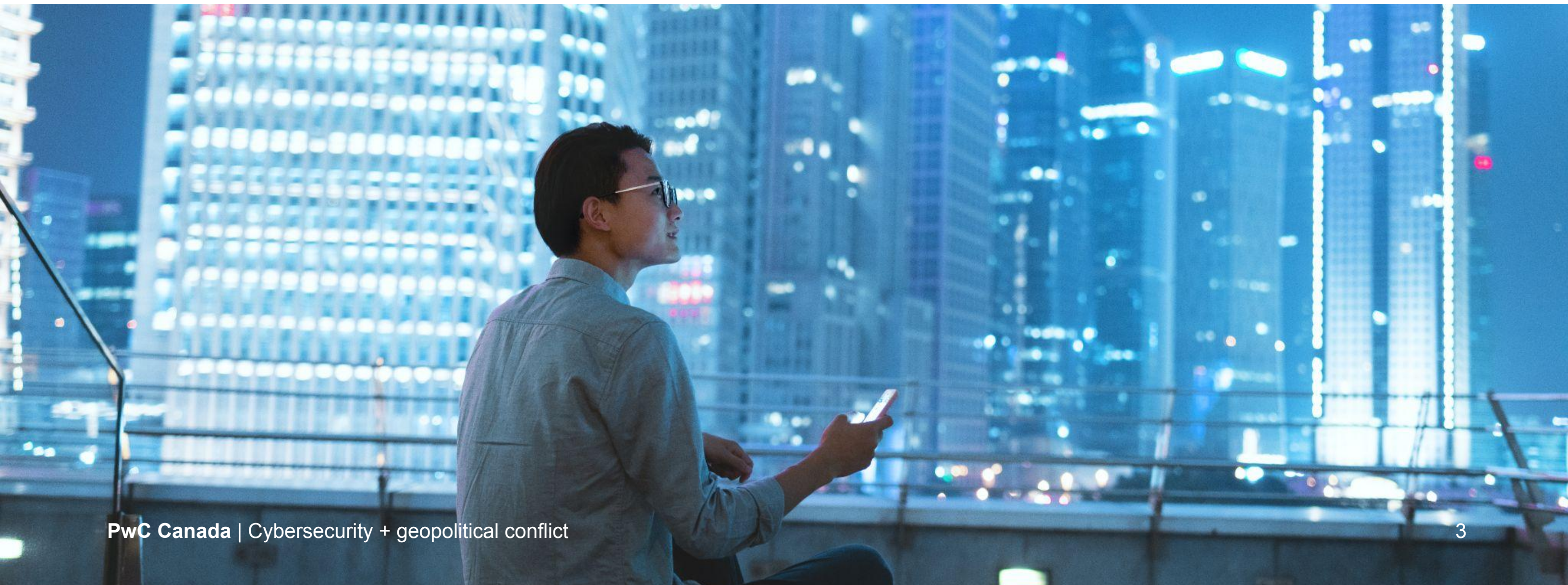


Question: *How concerned are you about the following global threats negatively impacting your company over the next 12 months? (Showing only 'very concerned' and 'extremely concerned' responses)*

Source: *PwC, 25th Annual Global CEO Survey, January 2022.*

Four lessons learned from previous attacks that should inform companies' responses today

Lessons from prior geopolitical events	Implications for today
Multinational and global organizations can be affected even if they're not directly targeted.	Organizations with ties to the targeted nation or enterprise must monitor their computer network connections into and out of the country. They should review the risk of maintaining connectivity against their risk appetite. Some organizations might even consider a temporary shutdown as a preemptive measure, ahead of a geopolitical event.
Cybersecurity has become part of the arsenal in geopolitical conflicts, and threat actors can be sophisticated and persistent.	In times of crisis, organizations need to lower the thresholds for detecting intrusions. Ignoring what would be considered a false positive during a period of relaxed tensions might be particularly risky now.
Attackers often gain a foothold by stealing credentials like account names and passwords and then move unimpeded between systems (i.e., lateral access).	Organizations should be on the lookout for an uptick in spear phishing and social engineering to gain credentials.
The NotPetya attack spread around the globe, shutting down systems with such speed (hours, not days), thanks to automation.	Organizations should review their risks continuously, relying on near-real time network traffic analysis for swift threat identification and ramping up capabilities for quick reaction to threats.



What should boards and CEOs be doing about heightened cyber risks now?

We recommend that boards make time to review their organization's cyber posture as soon as possible. CEOs and senior management need to know where to shore up weaknesses.

Boards and CEOs should arrange for table top exercises with their CISOs to get a taste of what the organization is up against and how the security team defends against them. These exercises can be very effective in quickly educating boards and CEOs and giving them the confidence to decide and act.

What to ask your CISO and CIO

1. How exposed are our systems, people and assets in countries that are targets of attacks? How closely are we monitoring the connections into and out of those countries in our corporate systems?
2. What's the plan if we decide that we need to disconnect our systems? How quickly can we do it without harming our operations and our people?
3. Do we have an incident response (IR) playbook? Have we done exercises to test it? When was the last time we tested our IR plan? Have we discussed actions if hostilities begin? What are those actions?
4. How sophisticated are our threat detection capabilities? Are we able to detect intrusions in real time? How well do we monitor the cross-over from our IT systems to the tech that runs our operations?
5. Do we have strong relationships with national and/or local government agencies focused on cybersecurity? Have we contacted them regarding additional intelligence? How involved are we in industry or private-sector groups that share information with the government? How do we distinguish between accurate information and the disinformation and leaks that nation-state actors often deploy?
6. How well do our employees help protect the organization against theft of account names and passwords via phishing and social engineering? When did we last scan our systems to detect unauthorized (even if dormant) access?
7. How good are our foundational cybersecurity capabilities? What is the state of our organization's cyber hygiene?

What should cause boards and CEOs to take additional steps?

Boards and CEOs must plan for a stepped-up response commensurate to the much riskier cyber environment associated with a geopolitical event.

The situation is much riskier because there are no norms that govern cybersecurity globally — and this new environment would challenge what few self-imposed guardrails exist because it changes incentives for defenders and attackers.

CEOs and boards will have to consider more consequential questions. Should we disconnect and isolate the systems that are in the war zone? Can we continue to tolerate the risks or accept a reduction in functionality or capability in certain territories? Should we accelerate key mitigating measures that will require a reprioritization of resources?

What should CISOs be doing?

Consider all available resources including those from government agencies that provide a reasonable and foundational checklist for all CISOs and their security teams.
For example, the Canadian Centre for Cyber Security issued a bulletin that urges Canadian critical infrastructure operators to raise awareness of and mitigate known cyber threat activity.

PwC Canada recommends that CISOs do the following:

1. Implement basic cyber hygiene.
2. Put your IR plan into warm mode, dust it off, or exercise it.
3. Drop thresholds for detection.
4. Make lateral movement harder and stop automated propagation. Computer network exploitation, not just computer network attacks, will likely escalate.
5. Use all available resources, including government agencies, to identify potential threats from various third party actors, particularly if you operate critical infrastructure. Contact appropriate government agencies and sound the alarm if you see suspicious activity.
6. Be on the lookout for spear phishing and social engineering that are targeting critical infrastructure and operational technology (OT).
7. Agree on the governance process to guide your company's response.

Bottomline

For boards and CEOs, headline-grabbing events — like this cyber-related, cyber-enabled geopolitical conflict — can be an occasion for meaningful reflection on cyber strategy and investments. CEOs can and want to make a difference for the cybersecurity of their organization. And boards want to exercise better governance over cybersecurity.

Speaking the language of business, CISOs can secure the cooperation and collaboration of senior executives who need to be part of any response and recovery for every aspect of their organization, including supply chain, general counsel, business continuity, investor relations and customer relations.

pwc.com/ca