Deloitte.

Insights and actions

Preparing your organization for elevated cyber threats posed by geopolitical conflicts

Cyberwarfare has become a common method of attack in geopolitical conflicts, primarily targeting government entities and critical infrastructure, such as power, utilities, banks, and communication networks. It is also important to recognize that organizations, regardless of size, must take an enhanced security stance especially considering geopolitical tensions, as cyber-attacks represent a growing and probable threat under these circumstances.

Whether an intended target or not, damage to an organization's data, infrastructure, and reputation can be significant. Beyond cyber attacks that are aimed at disrupting system availability and integrity, there is also the risk of disinformation campaigns, which can impede society's coordination in response to threats. The intent of these cyber attacks—typically denial of service attacks (DoS) and malware (although a variety of tactics may be leveraged)—can be to cause panic, confuse, and distract from the broader geopolitical situations and, in some cases, impede the ability to respond to these situations effectively. For example, cybercriminals may see geopolitical conflict as an opportunity to take advantage of the public's fears—aimed at psychological, political, physical safety, and/or economic concerns—and need for information by executing targeted cyber warfare campaigns. Similarly, opportunistic adversaries may exploit a desire for information to launch targeted phishing campaigns to extract sensitive personal and financial information.

To adequately respond and protect both commercial and government organizations, cybersecurity leaders and their support teams should consider probable types of attack; potential intended targets; threat actors including copycats or counteragents; and possible tactics, tools, and procedures (TTPS) as well as normal network activity patterns[1]. That baseline information can provide the foundation of data in order to prepare for and identify potential future assaults and may act as precursors to other forms of business disruption. While protection and prevention are critical components, cybersecurity and business leaders should also proactively collaborate to prepare for a security event from a sophisticated nation-state style adversary. Bolstering crisis response practices, including preparing to act decisively in an uncertain environment and to communicate with law enforcement, is essential to prepare for cyberwarfare threats.

A new precedent in supply chain attacks

Current situation at-a-glance

- Following the February 24, 2022, military invasion of Ukraine by Russia, governments and businesses around the globe are advised to be on high alert and prepared to respond to disruptive cyber activity.
- Experts now point out that the military invasion was preceeded by several notable cyber incidents, including deployment of wiper malware, distributed denial-of-service (DDoS) attacks on Ukrainian government websites and financial entities, and recurring defacement of multiple Ukrainian government websites. These incidents are thought to be organized and preplanned efforts that were executed with precision[2].
- Cyberattacks have been a key tool of Russian aggression in Ukraine since before 2014, when the Kremlin annexed Crimea and hackers tried to thwart elections.

Current impact to industry

- It is not completely clear yet how Russian cyberattacks might overlap—or even directly target—American businesses. However, the US Cybersecurity and Infrastructure Security Agency (CISA), part of the Department of Homeland Security, has issued a "Shields Up" warning to businesses noting that while there are "no specific threats to the US at this time," organizations of all sizes must be prepared for cyber attacks, whether they are directly targeted or not[3].
- Through "Shields Up" guidance, CISA is issuing key information and alerts for critical infrastructure owners and operators on identifying and mitigating the risks of influence operations that use mis-, dis-, and malinformation (MDM)[4].
- This guidance was further amplified by an issued warning from the White House on potential threats[5].

Businesses should focus on understanding and updating the systems they already have to bolster protections, while taking steps to protect against and minimize potential damage. In addition to following CISA's guidance, security teams should be on the lookout for warning signs of attack and consider security and crisis response preparedness activities in the days, weeks, and months to come. Initiating these processes can contribute to stronger security functions both in response to the current elevated threat levels and as part of building high-performing programs beyond the current conflict.

Where to start?

Leaders can build (and retain) trust in times of crisis, navigate the organization through multifaceted risk, protect the enterprise from adversaries, ensure resiliency, and provide vision to navigate uncertainty in this crucial moment in history. **Acknowledging the threat and taking steps to prepare and protect your enterprise are critical, as well as establishing proactive lines of communication with government and law enforcement.**

Protect your enterprise

Organizations should take steps now to update technical protections, communicate elevated risk levels with employees, and refresh processes to be ready in the event of an attack by considering the following steps:

Actions to prioritize: ● NOW ▶ NEXT

For security teams

Security functions

- ● Increase vigilance and proactively update indicators of compromise (IOCs) and confirm common vulnerabilities and exposures (CVEs) are fully patched; where possible, reduce digital footprints to mitigate exposure
- ● Confirm ingress and egress points between enterprise networks and the internet (pay particular attention to non-traditional environments such as remote access, cloud usage)
- ● Pay close attention to intel collection from government bodies and move rapidly to incorporate into security procedures
- ● Identify relevant local and federal law enforcement to report a cyber incident, as law enforcement and/or government involvement/intervention may be necessary in the event of a potential state-sponsored attack
- ▶ Revise Incident Response (IR) playbooks, especially around Data Destruction and Recovery and Crisis Communications, to ensure they are up to date. Update playbooks to include scenarios for destructive malware, Domain Name System (DNS), Border Gateway Protocol (BGP), and multiple simultaneous attacks
- ▶ Confirm (or expand) security operations coverage for 24x7, global support with proactive hunt threat hunting
- ▶ Practice your organization's ability to prevent, detect, contain, remediate, report, and recover from cyber attacks to confirm program capabilities and resilience

For other functions in collaboration with security teams

Operations functions

- ● Evaluate supply chain impacts associated with sanctions and determine vendors in your network at elevated risk for cyber incident, as supply chains are likely target of attacks
- ● Revisit disaster recovery and business continuity playbooks and ensure they are up to date (disaster recovery processes are especially important in preparing for ransomware threats)
- ▶ Determine supplier and customer interdependencies with organizations (and contractors) operating in impacted geographies to evaluate potential risks associated with lost connectivity to these parties
- ▶ Prepare crisis command and response teams to be ready to move quickly and systematically to execute contingency plans in the event of an incident

Legal and Risk functions

- ● Determine any security or digital risk implications of sanctions impacting vendors in your network
- ▶ Review your company's cyber insurance coverage policies (many do not provide coverage for nation-state incidents or acts of war)
- ▶ Prepare communication strategy to reassure key stakeholders in the event of an incident

Human Resources/ Talent functions

- ● Issue warnings to professionals about the potential for disinformation—and elevated risk of phishing—related to email links or news headlines from unknown or untrusted sources and establish one source of truth for internal communications.
- ● Evaluate shift schedules of security teams to confirm coverage while avoiding overstrain on teams to provide greater coverage during these periods of heightened risk - security teams are subject to talent shortages, burnout, and high turnover
- ▶ Evaluate security training of security personnel to determine opportunities to expand experiences for active adversary engagement through simulation exercises, cyber ranges, and advanced operator or threat hunting training
- ▶ Communicate proactively and regularly with employees on cyber hygiene reminders
- ▶ Conduct cyber awareness training for all staff, and update training as necessary to reflect common methods adopted by adversaries

Boards and Executive Leadership teams

- ● Create a cyber oversight committee to actively monitor the situation and establish oversight for cyber risk across the organization, promoting accountability, enforcement, and communication or risks and mitigation strategies
- ▶ Establish methods to keep a pulse on the security landscape through active industry group engagement, public private partnerships, and active threat intelligence and regulatory guidance monitoring
- ▶ Review a security dashboard of current communication, crisis, risk management, reporting, and IR plans and practice response with table-top exercises to test technical controls; process; governance; and executive, board, and external reporting

In addition to these steps, business leaders should be on the look out for signs and symptoms of attack to promote rapid response and containment.

Attack Indicators

Security teams and business leaders should be on the lookout for signs that your organization may be experiencing a cyber attack. Some common symptoms of attack may include:

- ❑ Slower than normal internet speeds due to a spike in external network traffic, or higher than normal internal traffic leaving your network
- ❑ Files have been unexpectedly encrypted, blocking your access to them, or they are missing altogether
- ❑ New programs running, security programs turning off or reconfiguring themselves, previously stable applications crashing suddenly
- ❑ New toolbars or extensions that haven't been installed by the user/organization
- ❑ Excessive antivirus warnings or antivirus logs missing
- ❑ Login issues, such as: password changes unexpectedly, accounts locked after excessive login attempts, accounts logging in at strange times or from strange places
- ❑ Increased number of phishing emails/scams/emails from external senders
- ❑ Customer or vendor complaints or disruption

While these patterns are useful indicators, it is also critical to consider other enterprise risks that could impact security posture—for instance, supply chain and vendor disruptions from global or multi-national operations are possible and may influence normal traffic patterns or crisis operating procedures. These factors require significant strategic executive engagement to keep security and risk indicators in lockstep so that organizations can be ready to respond effectively to attack.

Takeaways for executives

Things are not business as usual – there is heightened risk of nation-state attacks and opportunistic penetration of security defenses; executive leaders and boards should be actively engaged in monitoring the situation, resourcing security functions appropriately, and information sharing with industry and law enforcement

Protection will require elevated vigilance, which requires rapid tuning of technical defenses as well as proactive communication and stakeholder engagement. Employees are likely to experience attempted attack and can be a resource in early detection and prevention

Incident and crisis response playbooks may be impacted by global and multi-national supply chain disruptions – updating and executing playbooks, tuning security tools, and reinforcing awareness can help fortify security defenses for more resilient programs in the longer term

Offensive skillsets and experiences of security teams are critical to operate in cyberwarfare – many cyber operators have not had extensive simulation experience (or formal training in adversary engagement); continuing to evolve learning and development opportunities for cyber teams and related business functions will be required to keep pace with modern threats

Sharing intelligence proactively with peers, government, and industry is critical to collective strength of our defenses – updating security protections to reflect IOCs and rapidly addressing vulnerabilities is critical

Information sharing is imperative to collective protection during this time. **To stay up to date on the latest threat intelligence, Deloitte Risk & Financial Advisory is offering access to its threat intelligence portal and bi-weekly threat briefings at no cost to our clients.** For more information, please contact detectandrespondportal@deloitte.com.

Contact us

Deborah Golden
Principal
US Cyber & Strategic Risk Leader
Deloitte & Touche LLP
Tel: + 1 571 882 5106
Email: debgolden@deloitte.com

Curt Aubley
Managing Director
Detect & Respond Leader
Deloitte & Touche LLP
Tel: + 1 703 682 3996
Email: caubley@deloitte.com

Adam Thomas
Principal
Extended Enterprise Leader
Deloitte & Touche LLP
Tel: +1 773 677 1074
Email: adathomas@deloitte.com

Chris Ruggeri
Principal
Crisis & Response Leader
Deloitte Transactions and Business Analytics LLP
Tel: + 1 212 436 4626
Email: cruggeri@deloitte.com

[1]"Joint Cybersecurity Advisory Alert (AA22-057A): Destructive Malware Targeting Organizations in Ukraine." Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigations (FBI), February 26, 2022.
[2]"Next Generation Intel- Dynamic Adversary Intelligence: Understanding Russian Cyber Operations Against Ukraine." Deloitte Managed Extended Detection and Response (MXDR), February 2022.
[3]"CISA's "Shields Up" webpage.
[4]"CISA Insight: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure." Cybersecurity and Infrastructure Security Agency (CISA), February 2022.
[5]"FACT SHEET: Act Now to Protect Against Potential Cyberattacks." The White House Briefing Room. March 2022.