SHIELDS UP

While there are no specific or credible cyber threats to the U.S. homeland at this time, Russia's unprovoked attack on Ukraine, which has involved cyber-attacks on Ukrainian government and critical infrastructure organizations, may impact organizations both within and beyond the region, particularly in the wake of sanctions imposed by the United States and our Allies. Every organization—large and small—must be prepared to respond to disruptive cyber activity.

As the nation's cyber defense agency, CISA stands ready to help organizations prepare for, respond to, and mitigate the impact of cyber-attacks. When cyber incidents are reported quickly, we can use this information to render assistance and as warning to prevent other organizations and entities from falling victim to a similar attack.

CISA recommends all organizations—regardless of size—adopt a heightened cybersecurity posture.

Reduce the likelihood of a damaging cyber intrusion.

- Validate that all remote access to the organization's network and privileged or administrative access requires multi-factor authentication.
- Ensure that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA.
- Confirm that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes.
- If the organization is using cloud services, ensure that IT personnel have reviewed and implemented strong controls outlined in CISA's guidance.
- Sign up for CISA's free cyber hygiene services, including vulnerability scanning, to help reduce exposure to threats.

Take steps to quickly detect a potential intrusion

- Ensure that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior. Enable logging in order to better investigate issues or events.
- Confirm that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated.
- If working with Ukrainian organizations, take extra care to monitor, inspect, and isolate traffic from those organizations; closely review access controls for that traffic.

Ensure that the organization is prepared to respond if an intrusion occurs

- Designate a crisis-response team with main points of contact for a suspected cybersecurity incident and roles/responsibilities within the organization, including technology, communications, legal and business continuity.
- Assure availability of key personnel; identify means to provide surge support for responding to an incident.
- Conduct a tabletop exercise to ensure that all participants understand their roles during an incident.

Maximize the organization's resilience to a destructive cyber incident

- Test backup procedures to ensure that critical data can be rapidly restored if the organization is impacted by ransomware or a destructive cyberattack; ensure that backups are isolated from network connections.
- If using industrial control systems or operational technology, conduct a test of manual controls to ensure that critical functions remain operable if the organization's network is unavailable or untrusted.

Business leaders have an important role to play in ensuring that their organization adopts a heightened security posture. CISA urges all senior leaders, including CEOs, to take the following steps:

- **Empower Chief Information Security Officers (CISO:** In this heightened threat environment, senior management should empower CISOs by including them in the decision-making process for risk to the company and ensure that the entire organization understands that security investments are a top priority in the immediate term.
- **Lower Reporting Thresholds:** Every organization should have documented thresholds for reporting potential cyber incidents to senior management and to the U.S. government. In this heightened threat environment, these thresholds should be significantly lower than normal. Senior management should establish an expectation that any indications of malicious cyber activity, even if blocked by security controls, should be reported, as noted in the Shields-Up website, to CISA or the FBI.
- **Participate in a Test of Response Plans:** Cyber incident response plans should include not only your security and IT teams, but also senior business leadership and Board members. If you've not already done, senior management should participate in a tabletop exercise to ensure familiarity with how your organization will manage a major cyber incident, to your company and the companies within your supply chain.
- **Focus on Continuity:** Investments in security and resilience should be focused on systems supporting critical business functions, identifying those systems, and conducting continuity tests to ensure critical business functions can remain available subsequent to a cyber intrusion.
- **Plan for the Worst:** While the U.S. government does not have credible information regarding specific threats to the U.S. homeland, organizations should plan for a worst-case scenario. Senior management should ensure that exigent measures can be taken to protect your organization's most critical assets in case of an intrusion, including disconnecting high-impact parts of the network if necessary.

As the nation's cyber defense agency, CISA is available to help organizations improve cybersecurity and resilience, including through cybersecurity experts assigned across the country. In the event of a cyber incident, CISA is able to offer assistance to victim organizations and use information from incident reports to protect other possible victims. All organizations should report incidents and anomalous activity to CISA and/or the FBI via your local FBI field office or the FBI's 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov.

To connect with your local Cybersecurity or Protective Security Advisor here in Region 2 (NY, NJ, PR, and the USVI), please contact:
Rich Richard at richard.richard@hq.dhs.gov (Cyber) or Mark Kreyer at mark.kreyer@HQ.DHS.GOV (Protective)

For media enquiries in Region 2, please contact Dannette Seward at dannette.seward@cisa.dhs.gov

ADDITIONAL RESOURCES

Visit Shields Up | CISA and Shields Up Technical Guidance | CISA for regular updates to these resources.

CISA Resources

Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure (March 2022)

CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure (pdf) (February 2022)

CISA Insights: Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats (pdf) (January 2022)

Alert (AA22-011A) Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure (January 2022)

CISA Insights: Preparing For and Mitigating Potential Cyber Threats (pdf) (December 2021)

Reminder for Critical Infrastructure to Stay Vigilant Against Threats During Holidays and Weekends (November 2021)

Russia Cyber Threat Overview and Advisories

CISA Tools

COVID-19 Disinformation Toolkit

Free Public and Private Sector Cybersecurity Tools and Services

Mis-, Dis-, and Malinformation

Planning and Incident Response Guide for Election Officials

MDM Rumor Control Page Start-Up Guide
War on Pineapple

External Resources

RESIST 2 Counter Disinformation Toolkit - GCS (civilservice.gov.uk)

Swedish Civil Contingencies Agency (MSB) | Countering Disinformation

StopRansomware.gov