March 2, 2022

Workiva’s response to Russia’s attack on the Ukraine: Volatile times call for heightened cybersecurity preparedness.

Workiva closely follows the guidelines published by the U.S. Cybersecurity & Infrastructure Security Agency’s (CISO) SHIELDS UP initiative, and has committed to sharing any incidents or anomalous activity to the proper law enforcement authorities in the jurisdiction(s) where the activity occurs.

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.

- Workiva requires all Workiva constituents to use Single Sign On with Multi Factor Authentication. Workiva recommends our customers to implement Single Sign On.

Ensure that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA.

- Workiva utilizes automated patching mechanisms to ensure that host and container software is patched and up to date. Vulnerabilities identified in 3rd-party libraries included in our application are prioritized by severity and patched as part of our SDLC.

Confirm that the organization’s IT personnel have disabled all ports and protocols that are not essential for business purposes.

- Workiva has established and documented our configuration settings in line with Center for Internet Security (CIS) baselines and SCAP compliant checklists.

If the organization is using cloud services, ensure that IT personnel have reviewed and implemented strong controls outlined in CISA's guidance.

- Workiva has achieved FedRAMP Moderate and ISO 27001:2013.
- All Workiva access is based on least privileged and requires the use of unique IDs with adherence to our password policies, including the requirement of Single Sign On and two-factor authentication. Access must be approved by the functional manager and system

owner as managed through our ticketing system. All activity within Workiva's network and systems are logged to our centralized SIEM tool.
- Workiva utilizes email spam filtering and blocks any automatic forwarding of emails, additionally devices and servers run anti-malware tooling. Employees undergo monthly social engineering assessments.

Sign up for CISA's free cyber hygiene services, including vulnerability scanning, to help reduce exposure to threats.

- While Workiva is not eligible for CISA's services (not a critical infrastructure provider), Workiva is FedRAMP Moderate. Additionally Workiva provides customers third party reports by PCI/CREST authorized providers to perform external scanning and testing on a semi-annual basis in addition to our internal scans and testing.

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.

- Workiva utilizes our security information and event management (SIEM) system to provide continuous monitoring and log analysis. Workiva's Information Security Team reviews logs and alerts for performance and security considerations including logs relating to authentication, endpoint, web application, and more. Logs are stored on a central logging system, transmitted over an encrypted channel, encrypted at rest, and segregated from other systems and users. Logs cannot be modified once written and deletion of log is monitored. Log information collected includes information such as time, data size, response latency, transaction type, web service method invoked, user/account/service information, hostname/ip, action and/or resources involved. Logs are continuously monitored for abnormalities and investigated per our standards and policies. Our alerts are continuously reviewed for accuracy, coverage and effectiveness and playbooks are developed and maintained to standardize and improve response. This data is used to perform investigations of reported security events and incidents.

- Activities within a customer organization are available to them on demand, more information can be found on our help site: https://support.workiva.com/hc/en-us/articles/360035646392-View-Organization-Activities

Confirm that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated.

- Workiva's devices and servers are protected by anti-malware software with real-time protection and updates enabled.

If working with Ukrainian organizations, take extra care to monitor, inspect, and isolate traffic from those organizations; closely review access controls for that traffic.

- Workiva does not have any operations in Ukraine.

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.

- Workiva's Information Security team recognizes the need to be alert to external risks and is vigilant in looking for potential issues. We also employ active monitoring of key information used to identify threats.
  Workiva maintains an Incident response plan that addresses
  - Identification
  - Documentation
  - Isolation
  - Resolution
  - Communication
  - Escalation

Assure availability of key personnel; identify means to provide surge support for responding to an incident.

- Workiva maintains a 24/7 support team with on-call paging to the relevant teams which is tested annually as part of our business continuity and disaster recovery testing.

Conduct a tabletop exercise to ensure that all participants understand their roles during an incident.

- Workiva conducts quarterly table top exercises in addition to annual business continuity and disaster recovery testing to ensure teams are well versed in Workivas plans and know their respective roles.

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.

- Workiva utilizes redundant data backup in order to provide point-in-time recovery. In addition, Workiva allows customers to self-administer their accounts. At any time a customer can save/export a document or delete a document. Workiva supports saving

files in DOCX (MS Word), XLSX (MS Excel), or PDF (Adobe) formats for archiving on their own systems.
- Customer Tools: https://support.workiva.com/hc/en-us/articles/360035639692-Prepare-for-the-Unexpected

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.

- Workiva does not utilize industrial control systems.
- By implementing the steps above, all organizations can make near-term progress toward improving cybersecurity and resilience. In addition, while recent cyber incidents have not been attributed to specific actors, CISA urges cybersecurity/IT personnel at every organization to review Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure. CISA also recommends organizations visit StopRansomware.gov, a centralized, whole-of-government webpage providing ransomware resources and alerts.
- 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.

Additional Resources

- **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)**
- **COVID-19 Disinformation Toolkit**
- **Mis-, Dis-, and Malinformation (MDM) Planning and Incident Response Guide for Election Officials**
- **MDM Rumor Control Page Start-Up Guide**
- **Russia Cyber Threat Overview and Advisories**
- **Free Public and Private Sector Cybersecurity Tools and Services**
- **War on Pineapple**
- **External Resources**
- **RESIST 2 Counter Disinformation Toolkit - GCS (civilservice.gov.uk)**
- **Swedish Civil Contingencies Agency (MSB) | Countering Disinformation**