Following the Russian invasion of Ukraine, the Cybersecurity and Infrastructure Security Agency (CISA) announced a warning to all U.S. organizations to keep their “shields up” in anticipation of malicious Russian cyber activity. Among troves of guidance, what is the bottom line?

Agencies with OT/ICS environments are often in the very early stages of their OT cybersecurity journey. There’s a lot of complexity, as more and more devices become interconnected and interdependent. The threat is real, but the defense can get ahead of the challenge, and ShieldsUp has helped to amplify the challenges of our constantly evolving cybersecurity landscape.

**Action Items for All Organizations**

**Lessons for Leadership**

**Ben Miller,** VP of Services

"Reduce Risk"

- Strengthen cloud practices:
  - Regularly review/monitor:
  - Detect risk:
  - Respond to risk:

**Maximize Resilience:**

- Implement conditional access policies
- Actively review for anomalous activity
- Establish blame-free employee reporting
- Focus on staff awareness and training
- Establish baseline for normal activity
- Designate a crisis-response team
- Test backup procedures
- Define incident and roles/responsibilities
- Practice with a tabletop exercise

**If Working with Ukrainian Organizations, Take Extra Care**

- Authorize Chief Information Security Officers (CISO)
- Lower reporting thresholds
- Participate in response plan testing
- Consult CISA’s Ransomware Response Checklist
- Focus on continuity of vital work
- Plan for the worst-case scenario

Report anomalous cyber activity and/or cyber incidents to report@cisa.gov or (888) 282-0870.

**Footnotes:**

¹ CISA Shields Up

² Strengthening Security Configurations to Defend Against Attackers Targeting Cloud Services

³ CISA Ransomware Guide