CORL technologies

PREPARING VENDORS FOR CYBERWAR

Vendors servicing the healthcare industry are scrambling to adjust their cybersecurity preparation and response capabilities in the wake of potential cyberattacks stemming from the ongoing conflict between Russia and Ukraine.

Healthcare organizations and vendor risk management programs must provide support and reinforcements to help vendors remain vigilant in their cyberwar preparation and response capabilities.

Make Preparations for Cyberwar

- ✓ Identify assets in conflict zones
- ✓ Confirm which products, services, and applications are affected
- ✓ Backup data and code to safe locations
- ✓ Identify if any development resources are located conflict regions
- ✓ Review historical risk assessments for exposures with key controls
- ✓ Identify and inventory fourth-party vendors that may be impacted
- ✓ Establish a proactive communication plan with customers
- ✓ Review and validate access rights including privileged access
- ✓ Establish and empower CISO and cybersecurity teams
- ✓ Plan for worst-case scenarios

Monitor the Latest Threats & Attack Vectors

- DDoS
- Brute-force
- Ransomware
- Hacktivist attacks
- Destructive malware like WhisperGate and HermeticWiper
- Phishing
- Defacement
- Economic sanctions

Focus on Key Cybersecurity Controls

- Logging and monitoring
- Business continuity
- Disaster recovery
- Network controls & segmentation
- Cloud configurations
- Incident response planning and testing
- Patching and scanning including known vulnerabilities like Log4j
- Endpoint protections
- Multifactor Authentication (MFA)

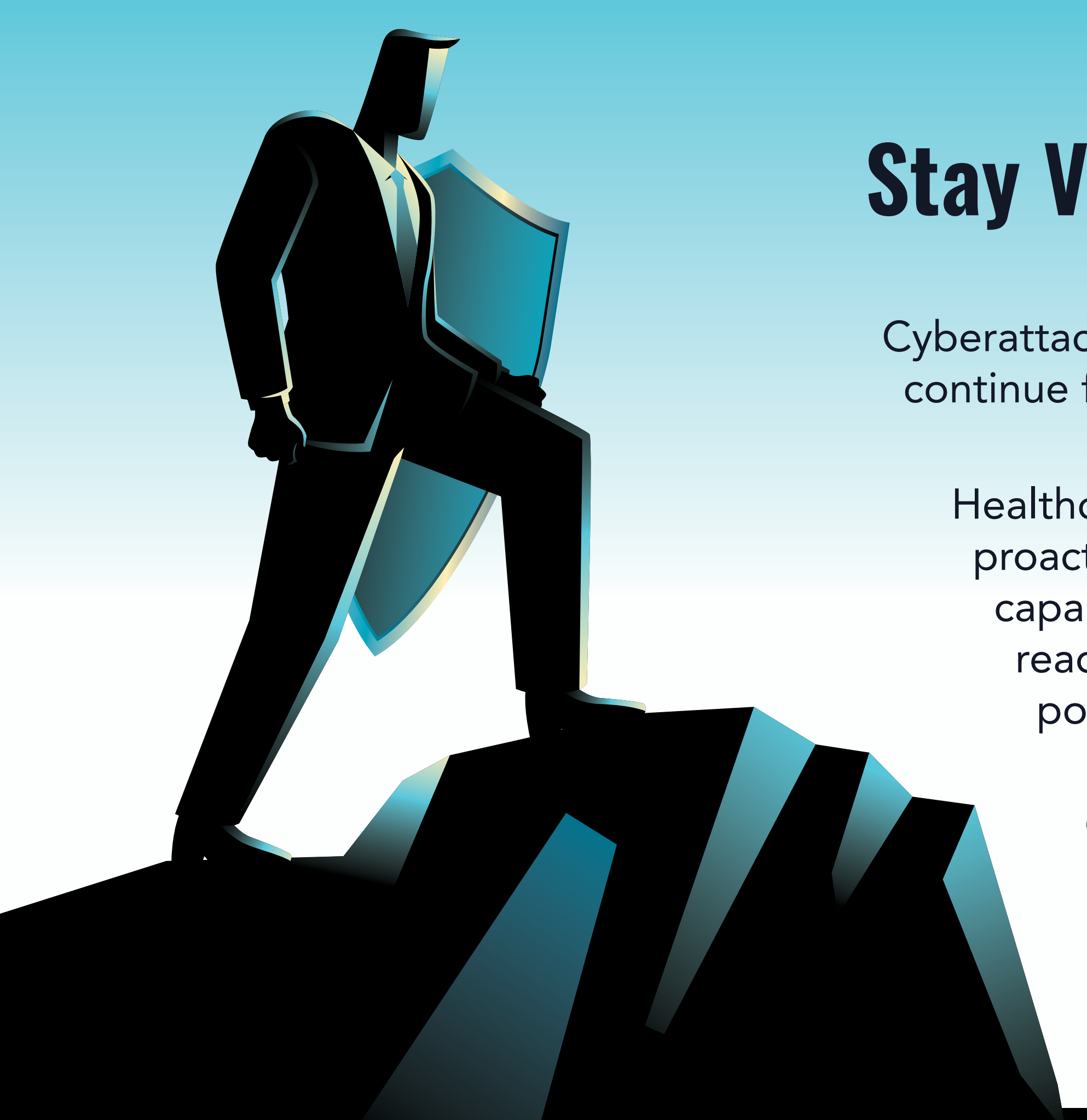
Engage Cyberwar Response Tactics

DESIGNATE a crisis response team

DOCUMENT a formal incident response plan

CONDUCT cyberwar tabletop exercises

ENSURE availability of staff and plan for surge capacity



Stay Vigilant

Cyberattacks stemming from the Russian invasion of Ukraine are likely to continue for some time as the conflict escalates.

Healthcare organizations and their vendors must continue to make proactive investments in cybersecurity defense and response capabilities. Organizations must maintain a heightened state of readiness to combat the growing threats of ransomware and the potential for escalations in cyberwarfare in the months ahead.

CORL will continue to monitor the situation in Ukraine and provide guidance and resources for the healthcare industry and vendor risk management programs as this crisis evolves.

About CORL Technologies

- **80,000+ vendors** already assessed and managed in CORL's vendor risk data exchange
- **130+ Organizations** using CORL's supply chain security managed services
- **Automated** assessment processes and reporting
- **Save** time, money, and resources
- **Scale your program** to cover your full vendor portfolio
- **Accelerate** assessment turnaround times
- **Protect and enable** the business
- **Be prepared and get protection** from supply chain breaches

CORL is a leading provider of tech-enabled managed services for risk management and compliance for healthcare organizations. CORL gets results by scaling organizational and vendor risk programs through our healthcare vendor clearinghouse, dashboard reporting that business owners can understand, and proven workflows that drive the organization to measurable risk reduction. Visit corltech.com and follow us on LinkedIn.

VISIT CORLTECH.COM AND FOLLOW US ON LINKEDIN

CORL technologies