How to Prepare for Cyberwar: 20-Point Checklist for Protecting Your Business

MRK technologies

Cybersecurity is top-of-mind amid the Russia-Ukraine conflict, with the threat of cyberwar becoming an imminent threat that could extend to EU and NATO member states — including the United States. As Russia-based cybercriminals become emboldened by Russia's actions, they will increasingly target businesses with profit-driven attacks like ransomware, phishing and more.

Organizations of all sizes should adopt a heightened posture when it comes to cybersecurity and protecting their most critical assets — not only during this time of increased uncertainty, but also on an ongoing basis.

Use this checklist to armor your business and continually mitigate risks of cyber attacks.

Technical Controls

- ☑ Enable multi-factor authentication (MFA) wherever possible
- ☑ Make sure you are up to date on the most current updates and patches (Microsoft, third-party applications, networking and wireless equipment)
- ☑ Block Russian .ru domains completely in web and email if not doing business there
- ☑ Add HermeticWiper, Distributed Denial of Service (DDoS) attacks and Russia-Ukraine Indicators of Compromises (IoCs) to your systems
- ☑ Block GEOIPs in countries your organization doesn't do business with or in, blocking on ingress and rejecting on egress
- ☑ Limit risky protocols over B2B VPNS such as SSH, RDP, MSSQL, SMB, MSRPC, LDAP, WINRM
- ☑ Turn on netflow on network devices if possible (aim for 90 days)
- ☑ Prevent users from installing device drivers
- ☑ Review any connections to third parties and potentially turn off any that may not be required
- ☑ Establish a process for turning off Business-to-Business VPNs
- ☑ While threat levels are higher, turn up security controls sensitivity for spam/phishing
- ☑ Look for ways to identify anomalies through UBA and network traffic analysis, particularly across B2B connections

Non-Technical Controls

- ☑ Test generators
- ☑ Review disaster recovery/business continuity plans and test recovery processes
- ☑ Review incident response plans and perform tabletop exercise to test preparedness
- ☑ Raise awareness, schedule ongoing awareness training sessions
- ☑ Instruct employees not to click on strange emails, links, requests or give up credentials
- ☑ Schedule ongoing awareness training sessions across your entire organization
- ☑ Review in-house and outsourced teams to identify users in high risk areas such as Russia and the Ukraine. Consider whether to keep this access active for the short-term.
- ☑ Review business partners to identify whether any are likely to be at higher risk due to the current climate in Europe. Consider whether this changes network or application access you wish to grant high-risk partners, or otherwise changes how you interact for the short-term.

Get Help from an Experienced Managed Services Partner

Security threats are always on the horizon—and changing every day. Now is the time to re-evaluate your cybersecurity measures and take proactive steps to prepare for potential risks.

If you want to ensure your organization is protected from cyberthreats large or small but are not sure where to start, please give us a call. MRK has teams of CISOs, analysts and engineers available to help, whatever your security needs may be.

About the Authors

Chris Prewitt

Chief Technology Officer

As Chief Technology Officer, Christopher Prewitt helps develop security related products and services for customers at MRK Technologies. Chris also helps support customers develop security strategies to reduce and manage risk in areas of security, privacy, compliance and disaster recovery. He has over 20 years of experience in IT Security working in a variety of industry verticals. Previously, Christopher has held Chief Information Security Officer roles in Fortune 500/1000 space. Christopher received his MBA from Cleveland State University and holds the CISSP, CISM and several technical certifications, including CISSP, CISM, OSCP, CEH, ECIH and PCNSE.

Connect with Chris on LinkedIn!

Chris Clymer

Director & Chief Information Security Officer (CISO)

Chris Clymer leads the CISO practices at MRK Technologies and has more than 20 years of experience working in IT/IT Security roles such as Chief Security Officer, Manager, Analyst, Engineer, Developer and Assessor. He has worked across numerous verticals—each with unique challenges—including healthcare, finance, manufacturing, government, law enforcement and retail. Chris specializes in security management, risk management, governance, information security and information technology and has extensive certifications, including ISO 27001, CISSP, GPEN (GIAC), GWAPT (GIAC), and FAIR.

Connect with Chris on LinkedIn!

Connect with our team to see how we can help.

216.535.4100 | www.mrktech.com/contact

MRK < technologies >