Cybersecurity Solutions:
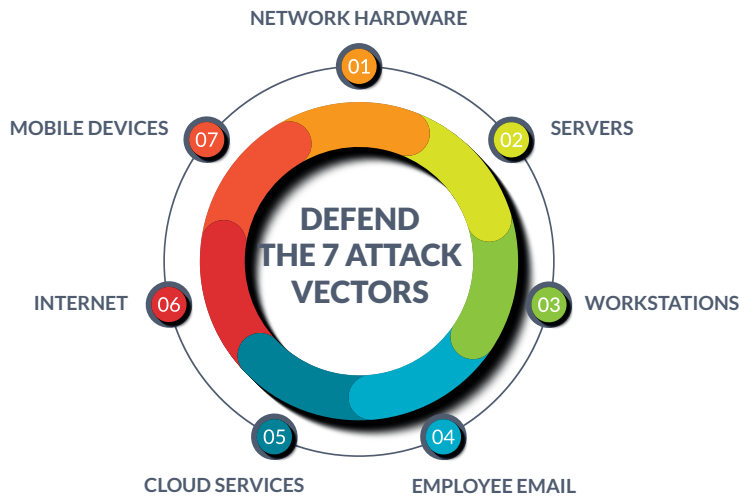# Why is Cybersecurity Important?

Utilities present a target like no other. One that hackers, data thieves and other cybercriminals find irresistible. Municipalities, energy companies, power grids – all have seen an explosion in cyberattacks over the past two years.

Malware infections increased by 358% through 2020. Ransomware attacks increased by 435% in 2020 compared to 2019. Because of this, the average cost of a data breach is now $3.8 million, assuming you can recover your operations at all.

SCADA systems and their peripherals are tempting targets for cyber criminals. They often contain vulnerabilities in the 7 Attack Vectors (shown below), which hackers can exploit to gain control of your operations.

Employing enterprise-grade cybersecurity solutions and continuous vigilance keeps these invaders out of your network and away from your mission-critical systems.

DEFEND THE 7 ATTACK VECTORS

- NETWORK HARDWARE — 01
- SERVERS — 02
- WORKSTATIONS — 03
- EMPLOYEE EMAIL — 04
- CLOUD SERVICES — 05
- INTERNET — 06
- MOBILE DEVICES — 07

Keep reading to learn how Mbroh can help!

Mbroh Provides Specialized Cybersecurity for Protecting Data Systems

Proper cybersecurity starts with knowing the location of vulnerabilities. This requires first-hand knowledge of remote network access, process automation, control systems, business systems, network equipment and security solutions.

Mbroh's Certified Information Systems Security Professionals (CISSP) take a comprehensive approach to cybersecurity, providing peace of mind for secured controls, business networks and applications.

Our team blends solid IT security expertise with practical experience in radio telemetry, microwave systems, PLCs and RTUs, field instrumentation, control system protocols, SCADA system usage, and business applications.

Our Services include:

Cyber/SCADA Vulnerability Assessments

- Internal and External Network Vulnerability Testing
- SCADA Testing
- Network Security Policy Review

System Design for Security

- Security Master Planning / Program Management
- Enterprise-Wide Security Policy Development
- Network Security Architecture Design
- Access Control Policy Development

Vulnerability Remediation

- Security Systems Configuration and Deployment
- Cybersecurity Awareness Training
- Network Segmentation Limiting Access to Mission Critical Networks
- Recommendations on Proven Network Equipment and Implementation

Cybersecurity Maintenance

- Network Hardware Software Patching/ Updates
- Network Vulnerability Testing and Remediation
- On-Call Network Consulting and Support

Contact us to start securing your systems!