Cyber Vigilance Checklist

If you check at least one box as a "NO," it is time to reconsider your cybersecurity posture – and begin exploring potential vulnerabilities in your IT infrastructure.

Assessment and Management of Risk

- [ ] Are you confident with your company's security process of managed threat detection and prevention?
- [ ] Does your IT department or MSSP provide cybersecurity through a balance of machine learning with human analysis?

Remote/Hybrid Workplace Security Strategy

- [ ] Has your IT team and/or MSSP clearly identified your cybersecurity program's value, roles, and responsibilities?
- [ ] Are your security program controls on network-dependent devices clearly defined and aligned in a roadmap that addresses organizational goals?

Communication with Stakeholders

- [ ] Do the right people in your organization grasp your security program processes for response to potential cyber threats?
- [ ] Does your IT team and/or MSSP have a clear plan of action to manage escalated alerts in a timely manner?

Infrastructure Management

- [ ] Do you have a next-generation firewall guarding your organization's perimeter?
- [ ] Do you have unified endpoint protection with detection and response across network, endpoint, and cloud assets?

Operational Management

- [ ] Can your IT team rely on a 24/7/365, U.S.-based, human-staffed Security Operations Center (SOC) to reduce response times and improve security outcomes with dedicated experts who are constantly monitoring your environment and investigating threats?

Cyber Maturity and Posture

- [ ] Is your cybersecurity program in an advanced "optimized" stage of maturity, with operational tasks automated and processes, policies, and controls working effectively companywide?
- [ ] Does your executive team have the data and reporting to clearly identify your cybersecurity posture as upright?