CYBER READINESS INSTITUTE

# Assessing the Right Type of Vendor: Your Risk

CYBER READINESS INSTITUTE

These questions will help you better assess and understand your cybersecurity risk.

| # | Question | Your Answer *(Yes or No)* |
|---|---|---|
| 1 | Do you collect and store Personally Identifiable Information (PII) of your customers (name, email, address, Social Security Number, age, gender, etc.)? | |
| 2 | Do you collect and store Protected Health Information (PHI) of your customers (medical history, medical test results, prescriptions, etc.)? | |
| 3 | Do you collect, store, process, or transmit any financial information of your customers (credit card numbers, bank accounts, etc.)? | |
| 4 | Do you have confidential or proprietary information belonging to your organization, customers, suppliers, or other partners on your computers? | |
| 5 | Could attackers use access to your organization's systems to reach a customer, supplier, or other connected organization? | |

| # | Question | Your Answer *(Extremely damaging, Damaging, Not very damaging)* |
|---|---|---|
| 6 | How damaging would it be to your organization if the information on your computer systems was lost or made publicly available? | |
| 7 | How damaging would it be to your organization's operations if your computer systems were unavailable for 72 hours (three days)? | |
| 8 | How damaging would it be to your customers or the community if your data was unusable or you were unable to operate? | |

**If your answers to the above are mostly "yes," your organization has a high level of cybersecurity risk. If you selected "damaging" or "extremely damaging" for data loss and business continuity, your organization has elevated cybersecurity risk.**



© 2026 Center for Global Enterprise (CGE). Cyber Readiness Institute is an institute of CGE. Free to use and share with attribution.