1. Identify. The organization should have an understanding of the cybersecurity risks it faces so it can prioritize their efforts.
2. Protect. This is about putting appropriate safeguards in place to protect data assets and limit or contain the impact of a potential cybersecurity event. This includes educating and empowering staff members within the organization to be aware of risks, establishing procedures that focus on protecting network security and assets, and potentially utilizing cyber liability insurance to protect a company financially in the event a cyber criminal is able to bypass the protections that are in place.
3. Detect. Outline the activities that assist in discovering the occurrence of a cyber attack and enable timely response to the event. In order to quickly and efficiently diagnose a cyber attack, companies should implement data classification, asset management, and risk management protocols that alert them when data appears to be compromised.
4. Respond. Document the appropriate actions that should be taken following the detection of cybersecurity threat. A company’s response should include proper and thorough communication with staff, shareholders, partners, and customers as well as with law enforcement and legal counsel as needed.
5. Recover. Determine how an organization can recover and restore any capabilities or services that were imparied due to a cyber attack.