

6 BASIC ELEMENTS OF CYBERSECURITY

As threats to organizational information systems and data become increasingly common, it is crucial organizations understand the basic elements of cybersecurity and the growing threats these cyberattacks pose.

LEADERSHIP & GOVERNANCE



Define the tone at the top. Companies must demonstrate due diligence and effectively manage the company's risk. Put policies and procedures in place to limit the risk to vulnerabilities.

HUMAN FACTORS

Train and educate. Provide educational materials and resources to employees and contractors. To ensure they understand the severity of being aware of the implications of a cyber-breach.



INFORMATION RISK MANAGEMENT



Controls and processes. Manage risk factors through assurances and frequently checked and monitored processes. Regular assessments are a part of any strong security plan.

BUSINESS CONTINUITY

Cyberattacks are real threats. Cybersecurity events need to be included in continuity plans. Cyberattacks pose just as much of a danger to organizations as anything else and have to be considered in a threat and risk analysis.



OPERATIONS AND TECHNOLOGY



Technology is always evolving. Operational strategy and technology work hand-in-hand. Inefficient technology means inefficient operation. Measure the controls and strength of technology to minimize the potential, or impact, of a security breach.

LEGAL AND COMPLIANCE

Laws and regulations change. It's imperative to stay up to date on regulations and standards. Many of these are put into place as a result of a previously significant breach in security.



Learn more about our Risk Management Practice and what we can do for your business.

833-683-7076 | www.schgroup.com