ASSESSING CYBER RISK

What are the Cyber Risks for my Business?

Cyber risk can be defined as the risk of financial loss, disruption or damage to the reputation of an organization through a failure of its information technology systems. Information technology has fueled rapid growth to small businesses, which can help you -- reach more customers, tap into new markets, grow faster, and create more jobs. With that increased reliance on information technology and access to data, new risks to your businesses' financial, customer data and reputation can occur. The process of cyber risk assessment includes identifying your organization's important data (financial data, customer data, and intellectual property), potential vulnerabilities for the systems that store or handle that data, and the potential impacts to your organization associated with a loss of confidence, integrity, or availability to that data.

Assessing and managing cyber risk is no different than managing other types of risk. If you were to manage the risk to your business from flood damage you would -- identify the most important assets that could be affected; consider how vulnerable those assets would be to a flood; consider the likelihood of flooding in the area; and determine what responses make the most sense based on the corresponding costs of responding to that risk. (Eg: invest in measures to protect those assets, move the assets, transfer the risk through insurance, or accept the risk.)

There are many available resources to assess cyber risk. How intensive an organization may decide to assess their cyber risks is based on a range of factors -- business priorities, regulatory standards or cost considerations. The National Cybersecurity Society (NCSS) provides a free survey that helps small businesses assess cyber risk called NCSS CARES (Cybersecurity Assessment and Resiliency Evaluation for Small Business). The assessment methodology was adapted from two main sources: The NIST Cybersecurity Framework and Carnegie Mellon's Software Engineering Institute, CERT, Resilience Management Model.

NCSS CARES measures small business risk based upon the level of maturity of the business' organizational cybersecurity and resiliency processes as defined by CMMI. CMMI (Capability Maturity Model Integration) is a process level improvement training and appraisal program, developed by Carnegie Mellon University. NCSS CARES can be found at: https://nationalcybersecuritysociety.org/tools, and at our website under tools/survey.

Assessing your cyber risk is an important consideration for any organization's overall evaluation of risks. Many insurance providers are using an assessment to set rates for policies and understanding and managing risks is a critical step in ensuring your business is resilient. Begin now by assessing your risk through the NCSS CARES.