MANN GROUP
CYBERSECURITY

A Cybersecurity Maturity Scale for Small Businesses

The concept of capability maturity levels was invented by the U.S. Department of Defense in the eighties. It is used to measure the level of formality, consistency and optimization of a process, often used in information technology and software development.

The standard five-level maturity model can be adapted as a tool to understand the various maturity levels of cybersecurity for small businesses. This paper introduces our contribution: The Small Business Cybersecurity Maturity Scale (SBCMS).

The SBCMS establishes 6 levels (0-5) of increasing cybersecurity maturity, using previous models as a template. Typical conditions for small businesses are outlined, so as to enable mapping any SMB to its maturity level. Recommendations at each step of the maturity scale are also presented. The goal of the SBCMS is to guide cybersecurity stakeholders within SMBs for effective cybersecurity decision making.

Small Business Cybersecurity Maturity Scale (SBCMS)

Maturity Level	Typical Small Business Attributes	Suggested Action for SMBs in 2020
0 - Absence	No significant attention paid to cybersecurity, minimal "shrinkwrap" software controls	Review risk appetite and allocate budget, create plan
1 - Initial	Some ad hoc cybersecurity spending and budget, and some controls are in place, but these are mostly not written down or consistent. Significant regulatory compliance risks (if applicable)	Complete a preliminary risk assessment and risk analysis, write down a risk plan for 2020
2 - Awareness	Budget and plan exist, with some documentation such as an in house risk assessment, but potential compliance gaps and unmitigated risks exist	Manage to risk plan and budget, improve capabilities and controls, improve policies and procedures. Obtain a 3rd party assessment if not done.
3 - Control	Cybersecurity budget and plan are being managed by the organization's security officer. Gaps and areas for improvement exist, but the organization's time and resources have prevented adoption	Write down and improve policies and procedures for security event management, incident management, event management, disaster recovery, business continuity, cybersecurity training, lifecycle management
4 - Mature	Fully managed cybersecurity program in place, with independent assessments or audits, compliant to regulatory standards	Improve workforce awareness and develop a culture of cyber hygiene, conduct regular training
5 - Optimized	Organization has a full cybersecurity program that is proactive and continously improving, with governance, feedback loops and threat hunting	Celebrate your success! You are the envy of your peers. Or are you dreaming and soon to wake up to reality?

Mann Group Cybersecurity provides cyber risk management services for small businesses in the Pacific Northwest. Reach us by phone at 360-388-1286 or email david@manngroupit.com to schedule a free initial consultation or visit manngroupit.com for cybersecurity news and information about us.