Navigating the terrain of business can be tough; product and labour costs, profit margins, taxation rules and regulations, and many more factors can plague a business throughout its operational life. Many of these pitfalls are well-known and guidelines already exist to assist business owners in picking a prescribed plan of action. However, when examining the facets of small to medium-sized businesses, one area that is often overlooked is that of cyber-security.

A relatively new danger to business operation; cyber-threats and hacking have come into their own in the last twenty five years. In the beginning it was only the large scale enterprise level businesses that paid the price for neglecting their digital security. At one time big corporations were the only targets on the horizon; as they were the only ones with IT infrastructure and sensitive data. Contemporary threats now target anyone and everyone; including small businesses and their respective information.

Today's threats include hacking, phishing, and malware of various forms. Make no mistake; no business is too small to avoid attack. There is a common misconception among small business owners that they can fly under the radar; that their data is not as attractive or lucrative enough to attract the attention of cyber-criminals. While this was the case in the past, today organizations are so steeped in the digital world, and threats are so diverse, that anyone can fall prey to attack.

Today's owners and managers should verse themselves in the spectrum of digital security. Education is the first step in safeguarding your business and your information. Proactively creating a series of policies and operational procedures will diminish the probability of an attack. Waiting until your data is held hostage by ransomware to take action is doing yourself and your business a disservice. Acting reactively within this sphere is most punishing, as many attacks can outright cripple a business or destroy all its data entirely: 60% of businesses that have suffered a major cyber-attack will go out of business within 6 months.[1]

Creating and maintaining guidelines for protection is important, but without disseminating that information to your employees, it might as well not exist. Employee education is the front-line defense against cyber-attack. When everyone knows how to identify potential threats, the risk is severely diminished. Maintaining a culture of constant vigilance and equipping employees with knowledge is paramount for owners and operators. This priority starts at the top and must be maintained. There are a series of best practices when it comes to creating a secure environment; effective password management, ability to detect phishing emails, regular digital infrastructure maintenance (patches, updates etc.), lockdowns of confidential or sensitive

[1] https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html

information, and safeguarding network access. This list is nowhere near totally comprehensive, but grants a soft outline in which to follow.

Even with all of these precautions, one must still realize that there is no full-proof plan or totally secure setup that can protect your data in its entirety. With this in mind, the most critical aspect of cyber-security is to have a contingency plan, which includes backing up your data. Creating a schedule of regular data backup will mitigate the severity should an attack occur. Data backups come in a variety of flavours and varying levels of effectiveness; from the lowly USB jumpdrive, to hard drive redundancy, and all the way to cloud-based solutions. Backing up data can be a manual process initiated by the user, or implemented regularly with automated software. This is by far the most valuable measure that anyone can take in safeguarding against not only potential digital threats, but this also great insurance in the event of catastrophic hardware failure.

Company information is not something to be taken lightly, and often creating policies or implementing backup plans is not a specialty of those who are employed in your business. Reaching out to a professional within this field is often a great approach, as their experience and level of expertise will facilitate positive change. There are a number of local companies that can not only help create policy, but execute action plans to protect your information. Vetting them through references, online reviews, and asking for credentials is a great way to narrow your selection and find the right person or company to help you in your mission. The security of your business and its information is vital to your continued success, and taking the appropriate steps to safeguard yourself from cyber-criminals is essential in our increasingly digital world.

Christopher Odecki

Evan Suntres

MC Business Solutions