Business Leaders Invest in the Future with SMB Cybersecurity Best Practices

Hackers looking for easy access to valuable data know that small to midsize businesses (SMBs) often skimp on security measures. Consequently, bad actors can cripple unprepared organizations, frequently gaining entry by compromising email. But savvy business owners protect business assets with SMB cybersecurity best practices.

SMB Cybersecurity Best Practices Start with Investment

Business owners lose sleep over cybersecurity, and for good reason. Nearly half of reported data breaches affected SMBs, and most SMBs lack the resources to respond effectively. But by planning ahead and addressing vulnerabilities before they get exploited, organizations ensure the best possible outcomes.

Begin with a security first mindset and a commitment to look at cybersecurity as an investment rather than an expense. As with any investment, a wise business owner starts by understanding the environment. Bring in a security professional with expertise in your industry to conduct a risk assessment before an incident occurs.

A good assessment will look at business processes and policies, as well as existing systems and security controls, and identify vulnerabilities. Businesses use the results of that assessment as a starting point to develop a solid security strategy moving forward.

Set Multiple Roadblocks Against Hackers, Beginning with Email Filtering

No one strategy or tool will guarantee safety from hackers. Email filters, for instance, can block a large percentage of dangerous emails and prove critical to a security program. But a sophisticated hacker can obtain credentials on the dark web and execute a spear phishing attack that slides under the barrier.

Consequently, a successful cybersecurity solution will involve multiple lines of defense. Some essentials include the following:

- **Email filtering** – Email remains the most common attack vector for hackers. Protect your organization with filters that scan for phishing, malware, and spam. With a good filter, organizations can block certain types of attachments or scan attachments and links for potential dangers.
- **Multi-factor authentication (MFA)** – A simple username/password combination provides inadequate protection against attack. With MFA, logon verification requires additional layers, such as facial recognition or a code from an authentication app.
- **Antivirus** – Protect every device with antivirus. And make sure to update your antivirus program frequently to protect against current threats.
- **Careful vetting of tools and vendors** – Look carefully at the tools you use. Know what functions they should serve and how to configure them properly. Likewise, know your vendors. Choose only reputable vendors with documented cybersecurity practices.
- **Continuous monitoring** – In addition to regular risk assessments, implement ongoing automated monitoring to flag anomalies before they turn into security incidents.
- **Backups** – Double-check your backup procedures to ensure regular, automated backups. Test backups frequently, make multiple copies and store a copy offsite.

Implement Well-Defined Policies and Procedures

In addition to tools, well-defined security controls and policies serve as the cornerstone of an effective security strategy. For instance, in a common spear phishing tactic hackers impersonate a CEO and send an email requesting employees to initiate a bank transfer. A simple procedure that requires verbal confirmation before a money transfer provides an effective solution.

Where possible, automate organizational policies. Well-crafted ePolicies can strengthen security while building compliance and reducing litigation exposure.

Never Underestimate the Importance of Security Awareness

No matter how many roadblocks you install, an email will always slip through the cracks. In the end, the organization's last line of defense rests with the users. Fortunately, targeted security awareness training can reduce successful phishing attacks and malware infections by up to 90 percent.

Effective end-user training will involve a multi-faceted approach, combining repeated formal training with just-in-time visual reminders and phishing simulations. Target training to the users' specific job activities. A security-first mindset drives effective SMB cybersecurity best practices.

Begin Implementing SMB Cybersecurity Best Practices Now

The security experts at Messaging Architects know the dangers that lurk in today's digital landscape. Putting off cybersecurity measures cannot be justified. From compliance risk assessments to ePolicy reviews and email filtering, they can help your organization build a solid cybersecurity strategy to protect vital business assets.