WHITE PAPER

Market Pulse

A Layered Approach Helps SMBs Protect Against Emerging Cyber Threats

Security posture is improved with a comprehensive strategy that includes managed services and cyber insurance.

Preparing for potential security threats is now an everyday part of business. In light of the damages that could result from a breach or attack, a security strategy is a must.

While most small and midsize businesses (SMBs) have the basics in place — including antivirus, spam filtering, and malware protection — most do not have a comprehensive security approach.

This is problematic. The attack landscape is changing rapidly. New threats, including those surfacing from the dark web and from within the supply chain, are challenging for SMBs to detect and address, especially for those with limited staffing.

A recent IDG survey among 121 IT decision-makers at companies with up to 1,000 employees examined their IT security strategies. The results reveal why a layered approach, including the use of managed services, helps improve companies' overall security posture and readiness for emerging threats.

Lack of a Holistic Strategy

Attacks against small and midsize businesses are escalating year over year, with 45% of SMBs saying their IT security posture is ineffective, according to a recent study from the Ponemon Institute.

That said, SMBs are taking action: they're leveraging a range of security strategies (see Figure 1), and the majority (80%) have a documented incident response or recovery plan in place.

However, security implementation isn't comprehensive; only 10% have adopted all of the strategies. Furthermore, just 24% of SMBs have adopted the three strategies that address today's emerging risks: dark web monitoring, third-party vendor breach alerts, and cyber liability insurance.

It's risky to ignore these new threats, according to Dr. Larry Ponemon, chairman and founder of the Ponemon Institute. "Cybercriminals are continuing to evolve their attacks with more sophisticated tactics, and companies of all sizes are in their crosshairs," he said, in a statement. "Every organization, no matter where they are, no matter their size, must make cybersecurity a top priority."

The Ever-Changing, Expanding Attack Surface

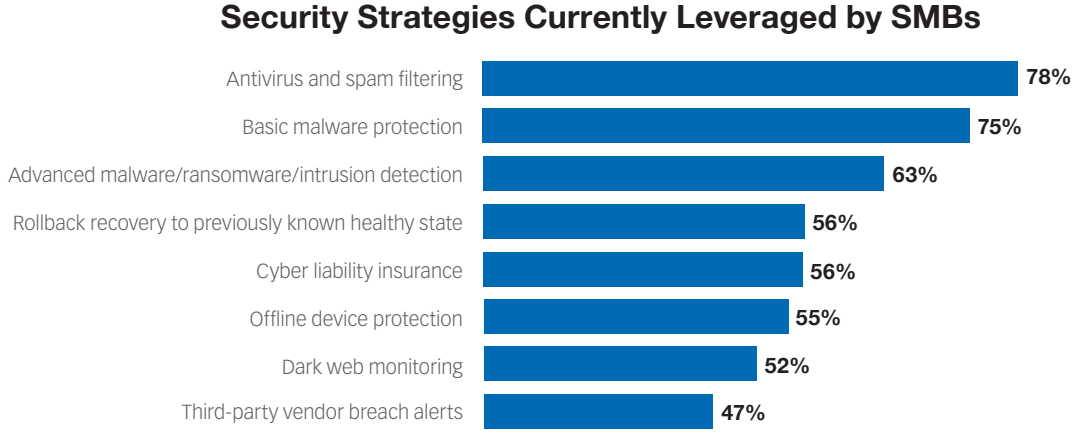
An effective security posture starts with recognizing that all companies have data that hackers covet — such as personally identifiable information (PII) found in employee or customer information systems. Social Security numbers, email addresses, and bank account numbers are just some of the PII that may be at risk.

Next, SMBs must be aware that the security landscape continually evolves. While ransomware and spam are still problematic, hackers have become more sophisticated. Their hacking efforts effectively result in a warehouse of stolen credentials for sale, sometimes hidden on the dark web, including usernames and passwords, that can be used to gain deeper access into a company's network.

"Dismissing the dark web as either too dangerous, too far out of the mainstream, or too complicated to merit attention does a disservice to the organizations that security professionals are responsible for protecting," writes Chris Dimitriadis, board member of ISACA.

Third-party risks are another area of concern. The Ponemon Institute found that 56% of organizations have

FIGURE 1



SOURCE: IDG, February 2020

reported data breaches caused by vendors' unsecure practices. As companies continue to digitally transform, their exposure to these supply-chain risks will increase.

Meanwhile, hackers are exploiting artificial intelligence and machine learning technologies to counter cyber defenses, effectively weaponizing the very tools companies use to improve their security posture.

All these factors point to the need for a holistic security strategy with multiple layers, as well as cyber insurance.

A Layered, Future-ready Approach

One big, monolithic security solution won't address the unique needs of individual organizations. Companies must take a layered approach that accounts for their potential exposure to threats as well as their appetite for risk. For example, some SMBs in highly regulated industries — such as healthcare or financial services — that have significant levels of PII will have different risk levels than a marketing or real estate agency.

A layered approach is effective because it addresses people, processes, and technology according to an organization's needs. For example, a typical company might start with security controls for organization-wide applications like Office 365 or email, then move on to end-user awareness and training, and then endpoint security for any points of entry (such as devices and equipment) to the corporate network.

The final layers should include considerations for cyber insurance and managed services, which fill gaps left by:

- Limited staff and expertise. Systems require constant monitoring for threats. In addition, security solutions generate data that must be analyzed — quickly — to weed false positives from verified threats. This requires significant time and effort, as new vulnerabilities continually emerge. Managed services providers have the deep expertise and committed resources to stay on top of these threats.
- Unknowns. Even with thorough risk assessments of third-party vendors, device and software vulnerabilities can be well-hidden. Both supply-chain risks and emerging threats from the dark web make it challenging for companies to effectively cover all their bases. In combination with managed security services, cyber insurance offers another layer of enhanced protection.

A layered security approach helps protect businesses from today's wide range of cybersecurity threats. Because the attack landscape is evolving so rapidly, it's critical to incorporate the appropriate levels of security and then lean on providers, including managed services, to fill in the gaps.