MSP cheat sheet for cybersecurity success

Quick tips to help you build cyber resiliency for your customers

In today's digital landscape, small and medium-sized businesses (SMBs) face an ever-evolving array of cyberthreats that can jeopardize their data. According to a recent TechAisle report[1], 85 percent of SMBs say that data security and data protection enable cyber resiliency and reduce business risk. Use these tips below to help your SMB customers build their cyber resiliency and safeguard their business against looming threats.

SMBs employ a range of security measures to protect their data, including:

- Perimeter defenses, such as firewalls and identity and access management.
- Systems to prevent unauthorized entry.
- Data safeguards such as encryption, password managers, and data loss.
- Prevention to protect information from internal and external threats.
- System security measures, such as antivirus software and data encryption.
- DNS protection to fortify corporate systems and virtual environments.

To build a robust data protection strategy and safeguard their business, SMBs are prioritizing these essential data protection measures:

- **Comprehensive backups:** Implement regular, reliable backups for all data, regardless of location (servers, cloud, endpoints).
- **Automated protection:** Employ email and endpoint protection tools to prevent data loss through malicious attacks.
- **Threat vector defense:** Strengthen your defenses against cyberattacks by implementing secure access service edge (SASE) and network access control (NAC) solutions.
- **Ransomware resilience:** Invest in dedicated ransomware protection to safeguard critical data.

Complementary to data security and protection is a robust cyberinfrastructure that empowers SMBs to detect and respond to threats proactively. Given the complexities of threat detection and response, many SMBs rely on specialized third-party providers.

SMBs typically employ a combination of technologies to detect and respond to cyberthreats. This includes tools for identifying vulnerabilities, recognizing attack patterns, and automating defensive actions. Breach detection systems and vulnerability scanners are widely used to identify potential risks.

Managed detection and response (MDR) services offer an alternative approach, providing comprehensive threat detection, investigation, and response capabilities. Additionally, threat intelligence can enhance an organization's ability to anticipate and defend against emerging threats.

Five steps to take to safeguard data as a business priority

1

Define your cyber strategy in business terms

Identify your most critical digital assets and assess the potential impact of a cyberattack on them.

2

Develop data security and protection as a core competency

Data security is most effective when combined with data protection. Automated protection against vulnerabilities and well-managed backups can safeguard your high-value data and business viability.

3

Bolster detect and respond capabilities

If you are not seeing cyberattacks, you need better threat detection. Once aware, you need to react quickly to stop or recover.

4

Increase effectiveness—reduce complexity

Platform-based security and strong partners can overcome integration challenges for cyber success.

5

Don't fall behind the cyber curve

Cybersecurity is not a "set it and forget it endeavor." Consider adopting always-on, up-to-date security solutions and managed services to stay ahead.

By implementing these best practices, you can help your SMB customers strengthen their cyber resiliency and defend their organization from emerging threats.

1 TechAisle, Why Cybersecurity Needs to Be a Business Priority Report, October 2024

opentext™