

SMB Security: A Growth Opportunity for MSPs

Introduction

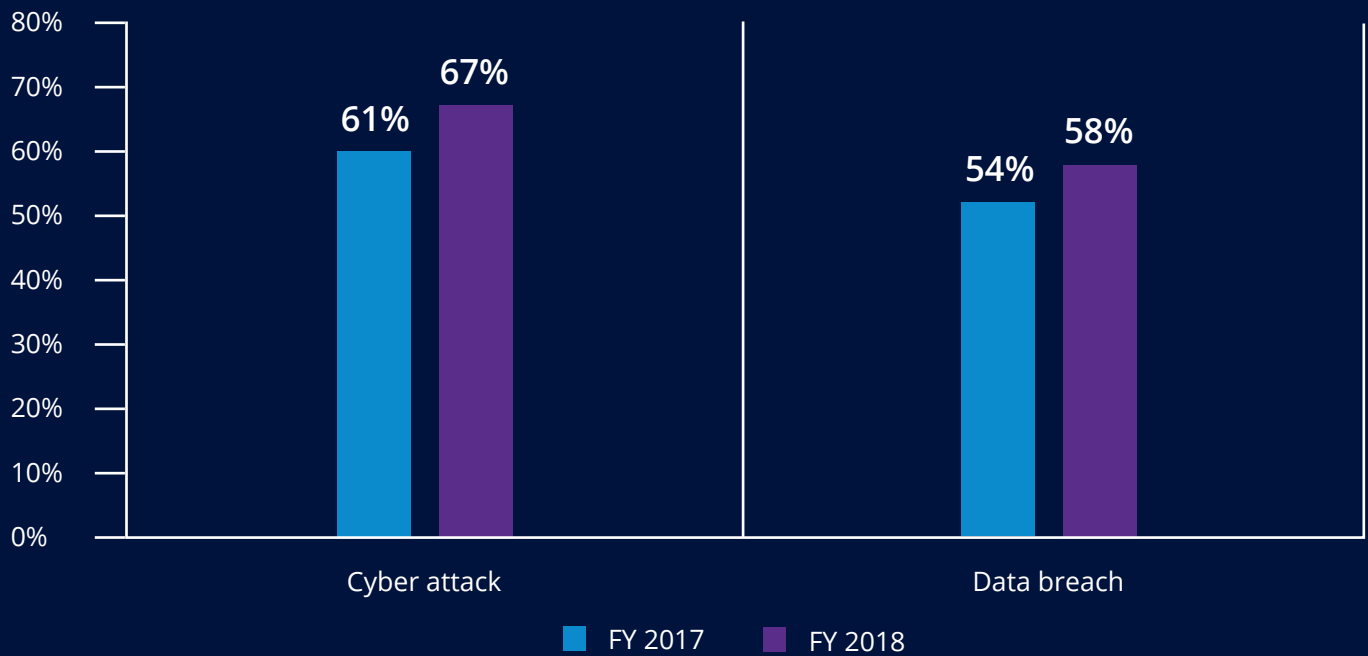
The statistics are staggering: Business email compromise (BEC) attacks are up 250% year-over year¹, it takes an average of 197 days to identify a data breach, and the average cost of a data breach is \$148 per record.²

Today, no organization can settle for bare-minimum security. In particular, small and medium-sized businesses (SMBs) need solutions that enable them to defend themselves with the same effectiveness as their mid-market and enterprise counterparts — which means managed service providers (MSPs) have a great opportunity to either add a security offering to their current portfolio or start down the path toward becoming a full-fledged managed security services provider (MSSP).

In this paper, we'll explain the security crisis SMB are facing and the resulting security service opportunity for MSPs.

Cyberattacks and the SMB

Industry research reveals that SMB organizations are experiencing more cyberattacks and data breaches than last year:



Source: Ponemon, 2018 State of Cybersecurity in Small & Medium Size Businesses

Cyberattacks and the SMB

Fending off these attacks can be more challenging for SMBs than mid-market and enterprise organizations — in fact, 58% of data breaches occur in small businesses.³ Factors include limitations in the following areas:



Budget

Smaller budgets mean that initiatives deemed important but not urgent, like IT security, often get put on the back burner.



Technology

SMBs tend to rely on basic tools like antivirus software and firewalls, and lack a comprehensive security solution.



Staffing

IT teams at SMBs are often small, sometimes just one person. A dedicated IT security specialist is a luxury that barely any SMB can afford.



Expertise

Internal IT staff are usually generalists with little proficiency in establishing and maintaining a strong security stance.

Moreover, even a single cyberattack can have devastating effects on an SMB. In one survey, 67% of MSPs reported that SMB clients suffering a cyberattack experienced a loss of business productivity and 50% reported them having business-crippling downtime.⁴

Adding Security Services to Your Portfolio

Despite the growing frequency and cost of cyberattacks, nearly half (47%) of SMBs say they have no understanding of how to protect their companies against them⁵ — which translates to a great opportunity for MSPs. By delivering security services, either as an addition to your current offering or as part of your transition to becoming a MSSP, you can realize all of the following benefits:



Additional Revenue Streams

Security services provide opportunity for both recurring revenue (through detection and protection services, such as continuous monitoring) and one-off revenue (through response and remediation services).



Differentiation

Customers will favor MSPs who offer security services in addition to other services, such as remote monitoring and management (RMM) or backup and recovery. And customers that want a service provider focused on security will be looking to an MSSP for answers.



Competitive Offerings

By offering security services, your business will be able to compete with other service providers who are already providing security services, enabling you to attract new clients and bring more value to current customers.

Choosing the Right MSSP Solutions

Of course, your security service offering has to meet your customers' needs. Be sure the solutions you choose assist with the following high-level goals:

01 | Implementing Your Security Practice

Adding on new services can place a burden on the MSP and the customer. Look for security solutions designed to help simplify the implementation of your security practice, so they add value from day one. This should include assessing the environment, identifying risk and delivering visibility, all without adding overhead.

03 | Putting Key Reporting In Place

Just as there are key metrics that show a business is running well, there are standard reports that can be used to identify and measure risk. Using those reports, MSPs can, for instance, reduce helpdesk SLAs and eliminate common security problems that keep techs from addressing more important issues.

02 | Understanding Where Sensitive Data Resides

Knowing where an organization's most sensitive data (both structured and unstructured) resides is the first step to securing it. Make sure your offering can help your customers identify and secure their valuable data. This functionality will serve as the foundation for all further data security services you provide.

04 | Achieving And Maintaining Compliance

Just like larger organizations, many SMBs are subject to mandates like HIPAA, CCPA, GDPR and PCI DSS. Make sure you can help your clients prove their compliance, either as part of your security offering or as a separate service.

Beyond these foundational elements, MSSPs can also offer more advanced security services, such as monitoring and threat detection, risk assessment and incident response.

Netwrix Solutions

Netwrix solutions can help your MSP build a solid security service offering by delivering:

01 | Data-Centric Security

Netwrix solutions start with the focus of attacks: data. Beginning with data ensures that the layered security strategy you build actually protects the organization's data from cyberthreats.

02 | Automated Risk Assessment

Netwrix solutions help you to understand the unique set of risks for each customer, which is critical for establishing and maintaining an appropriate security stance.

03 | Comprehensive Visibility

Netwrix solutions centrally audit activity across a wide range of data storages, systems, platforms and applications, including both on-premises and cloud applications and both structured and unstructured data.

04 | Easy Implementation

Netwrix provides technical training and certifications that ensure you can quickly implement our solutions, as well as sales training that provides a full understanding of our solutions and how they can help you make money by offering new services.

05 | Compliance Focus

Netwrix's data classification, auditing and reporting capabilities are mapped to nearly a dozen common regulatory mandates, which simplifies the process of achieving and demonstrating compliance.

Conclusion

Netwrix solutions provide MSPs with a unified and centralized approach to security, helping you understand where sensitive data resides, assess risk, monitor activity and prove compliance. Whether you're looking to add a new security service to your portfolio or transition from MSP to MSSP, Netwrix can help.

Used Sources

- 1 | BDO, 2018 Cyber Governance Survey.
- 2 | Ponemon, 2018 Cost of a Data Breach Study.
- 3 | Verizon, Data Breach Investigations Report (2018).
- 4 | Datto, State of the Channel Ransomware Report (2018).
- 5 | Ponemon, State of Cybersecurity in Small & Medium Size Businesses (2018).



About Netwrix

Netwrix is a software company that enables information security and governance professionals to reclaim control over sensitive, regulated and business-critical data, regardless of where it resides. Over 10,000 organizations worldwide rely on Netwrix solutions to secure sensitive data, realize the full business value of enterprise content, pass compliance audits with less effort and expense, and increase the productivity of IT teams and knowledge workers.

Founded in 2006, Netwrix has earned more than 150 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

For more information, visit www.netwrix.com.

Contact Us

Corporate Headquarters

300 Spectrum Center

Drive Suite 200

Irvine, CA 92618

Phones

USA: 1-949-407-5125

Toll-free: 888-638-9749

EMEA: +44 (0) 203 588 3023

netwrix.com/social

