Cybersecurity for Small and Midsize Businesses: A New Opportunity for Service Providers

Akamai

Intelligent Security Starts at the Edge

Cybersecurity for Small and Midsize Businesses: A New Opportunity for Service Providers

It's 2019, and small and midsize businesses (SMB) need and want cybersecurity. In a recent survey of 1,000 US small businesses conducted by GoDaddy[1] almost 50% of survey respondents reported suffering a financial loss due to hacking, with 13% saying the loss was greater than $5,000. Security is a global problem; a Cyber Security Breaches Survey conducted by the U.K. government[2] found 42% of all micro/small businesses identified a cybersecurity breach in the previous year. Given the similarities in the responses it's not unreasonable to conclude that small businesses with meaningful assets everywhere in the world are being targeted. This white paper will explore:

- SMB exposure on the internet, and unique challenges they face dealing with security threats
- How ISPs can help SMBs address their security exposure
- The market opportunity for SMB security, and how providers can build a business case

Cybersecurity Challenges Small Businesses Face

SMBs face security threats every day. They're attractive targets because collectively they have substantial economic value and often lack security expertise. SMBs are exposed to malware that can steal and offload finanancial information, customer data, or valuable intellectual property. They face phishing attacks that use sophisticated social engineering to trick users into downloading malware, or giving away credentials that can be used to access monetizable assets. Widespread use of intelligent devices (Internet of Things) introduces additional exposure business owners may not even consider. For more insights see a related Akamai paper: *SMB Threat Landscape*.

To give a sense of the impact on small businesses:

- Hiscox, a cybersecurity insurance provider, notes 47% of small businesses have suffered at least one cyberattack in the past year, and 21% have experienced two to four attacks
- A recent Enterprise Strategy Group survey finds 67% of small organizations experienced at least one cybersecurity incident over the past two years, with the most frequent causes being human error (35%), general lack of understanding about cyber risk (28%), and new IT initiatives (27%)
- According to Verizon, 92% of malware is delivered by email, and 58% of malware victims are small businesses

At the same time SMBs face exposure, the UK survey mentioned at the beginning of this paper also showed 26% of SMBs vs. 62% of larger businesses have formal security policies, and 19% of SMBs vs. 47% of larger businesses have cybersecurity training for staff. Yet 74% of senior managers in SMBs said cybersecurity is a high priority. Bottom line: Most SMBs don't have the "security muscle memory" larger organizations do, and it's getting harder for them to adequately defend themselves.

Bottom line: most SMBs don't have the "security muscle memory" larger organizations do, and it's getting harder for them to adequately defend themselves.

The SMB Security Opportunity

ISPs are well-positioned to help SMBs address their security exposure. They're already in an advisory role with an ongoing IT relationship, established contacts, and billing connections, so guidance from a trusted source is likely to be well-received. Security solutions are available that play to provider strengths, while meeting SMB requirements for ease of use, broad coverage of devices, and price points compatible with modest budgets. Providers can create an engaging subscriber experience to drive incremental revenues and increase affinity for their access service offerings.

Extrapolating from data published by TeleGeography, a leading market analyst firm that tracks ISP businesses worldwide, and a survey of providers' SMB-focused business units, Akamai estimates there are 65 million SMBs globally that use Internet access services. With access charges around the world ranging from $50 to $125 per month, and a 10% to 20% uplift ($5 – $25 per month) for foundational security built into the access service, a middle of the road total available market (TAM) is a little less than $12 billion per year (average of high and low end estimates).

Although it's a rough proxy, another supporting data point is Gartner Research's estimate that the broader enterprise security market exceeded $124 billion in 2019.[3] Enterprises have more complex IT environments, but SMBs have significant economic impact worldwide, and their collective spend is likely to be a noticeable fraction of enterprise.

Akamai Secure Business Transforming SMB Security

Akamai enables providers to take advantage of the SMB security opportunity. Akamai Secure Business is a new web security solution that provides DNS-based security defenses that are lightweight and scalable. It allows ISPs to deliver a foundational layer of protection for SMBs across fixed, mobile, and converged networks. Secure Business was developed from the ground up to be operated by ISPs either as in-network licensed software managed by a provider, or "as a service" managed by Akamai. As described in detail in a companion document: *"Data Science is Essential to Deter Today's Internet Threats",* DNS-based defenses can cover every device in an SMB facility, and be highly responsive to today's dynamic threats.

From a provider's perspective, Secure Business is designed to give providers full control. They can brand the service based on their corporate identity and objectives. Providers define the user experience, and specify service levels through APIs. They also determine the business model (premium offering, bundle, tiered service etc) and set pricing that's compatible with regional conditions. Akamai helps providers jump start marketing efforts with a "Go to Market" package that offers guidance and examples.

Secure Business was designed for SMBs, and the user experience was created for customers with limited expertise, time, and resources. There's no need to install any software, and all of the devices found in a typical business are protected. Business managers "set it and forget it", the service identifies and blocks malicious activity or unwanted content without intervention. All of these advantages contrast with traditional SMB security solutions, which are often repackaged and repriced products filled with features most SMBs aren't well-equipped to use, and thus benefit from.

As shown in the examples below, providers are considering many business models for Secure Business. They're also investigating fee-based offers of complementary services like anti-virus tools for customers that want to extend their security protections even further.

Business Case #1

A large North American provider with approximately 2,500,000 SMB subscribers created two security service levels to add to their access service as part of a bundle: Basic blocks malware and phishing activity for $9.95 per month, and Premium ($29.95 per month) builds on the basic offering with simple filters business owners can configure to block content that's unwanted in workplaces (acceptable use policies or AUPs). The provider used Secure Business Cloud to reduce time to market, and minimize internal operational overhead. They're targeting new customers initially, and plan to extend the offers to all of their SMB customers in 2H 2019. Discounts are offered on the premium package if subscribers sign up for three years. They expect the service will be profitable in year two.

Business Case #2

Another large North American provider with 500,000 SMB customers has developed two security service levels as part of their access service – an entry product for $19 per month and a premium product for $29 per month. This will be followed by a service based on SD-WAN technology targeting regional multisite restaurant and retail chains. The combined focus will make security fundamental to the service itself and thus make Secure Business a core element of their portfolio. Innovation like this is possible because Secure Business is completely network agnostic, and scalable.

Final Thoughts

Competitive pressures from peers are motivating ISPs to evolve beyond connectivity and offer incremental value-added services to sustain revenue growth. Security services are an obvious candidate since there's high awareness of the need for security protections. Presence and a trusted position in SMB market segments create an opportunity for ISPs to offer a foundational layer of web protection to reduce their customers' risk. SMBs are often an underserved market segment and resource limitations can predispose them to outsource services like security.

Akamai Secure Business is designed to be deployed as an ISP service and developed specifically for SMBs. The service "just works" without imposing a configuration or management burden on business managers. A graphical portal makes it easy to understand threat status and configure optional web content filters to implement acceptable use policies (AUPs). Deployment options (licensed and "as a Service") help providers align business and operational requirements.

Secure Business lets providers control the pricing strategy and business model, and define the branding and user experience based on regional requirements and aptitudes. To generate interest providers can inform SMB subscribers about the threat landscape and even offer insights into local conditions. An Akamai "Go to Market" package helps jump-start provider marketing efforts.

1 https://www.godaddy.com/garage/godaddy-small-business-website-security-report/

2 https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018

3https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019