Small Business Series powered by Techaisle

Straight-Line Technology:
Driving Small Business Returns from IT

The Transition Game: **Moving from Safe to Empowered**

techaisle
www.techaisle.com

Global Industry Analyst & Market Research Orgnization
SMB Data You Can Rely On — Analysis You Can Act Upon

The Transition Game: Moving from Safe to Empowered

In the first place…

Source: Techaisle, www.techaisle.com

Security matters to small (1-99 employees) businesses. A LOT. Technology is essential to productivity, to growth, to profitability – but it exposes SBs to potentially-devastating security breaches. A frequently-quoted statistic holds that "60 percent of small companies went out of business within six months of a breach."

So…security matters. But cybersecurity is a daunting challenge. Technology is so complex, and the threat sources so menacing, that many small businesspeople practice "security through obscurity:" they hope that attacks will be pointed at larger targets, and that they can find safety by keeping a low profile.

Unfortunately, there are enough hackers, scammers and cybercriminals to go around – and every conscientious small business owner needs to address security treats, as they act to safeguard their businesses against other threats (loss of customer trust, compliance with applicable laws and regulations, loss of financial solvency) to their businesses. Evidence suggests that small businesses have IT security on their agendas: a Techaisle global survey of small businesses found that **security is a critical concern for 73% of small businesses.** And a close look at the findings shows that the **other issues that are important – especially cloud and mobility – can't be implemented without an effective security approach.**

SBs understand that a security breach can quickly evolve to a business issue. Asked about the impact of a breach on their businesses, **nearly half of survey respondents stated that their customers' privacy would be damaged; nearly 40% believe that customer trust in their business would suffer, 34% see a breach as damaging company reputation, and nearly one-quarter report that a breach would substantially damage their bottom lines.**

Source: Techaisle, www.techaisle.com

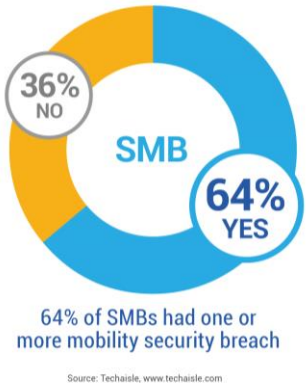
Security isn't just on a 'major issue' list with trust, compliance and financial viability – it is a key factor in defending against threats in these areas.

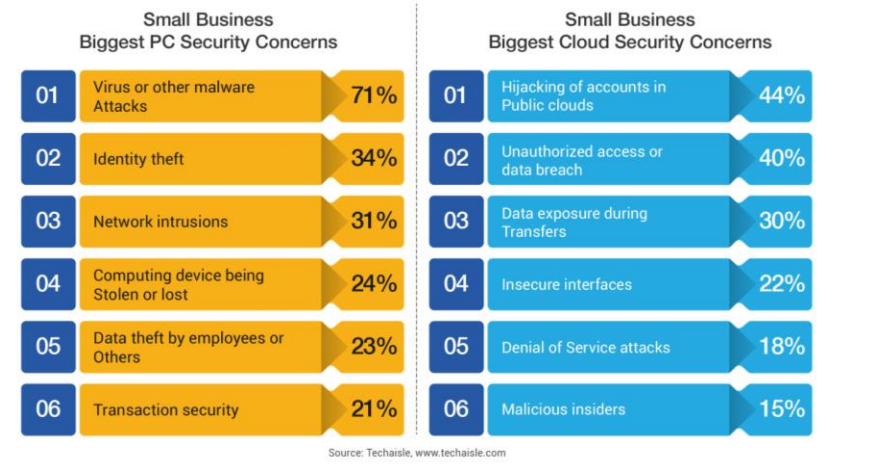
SB Security: defending against a wide range of threats

Small businesses – indeed, firms of all sizes – have a hard time establishing a starting point for IT security. They want to protect their data; they want to protect their users; they want to protect their networks; they want to protect the devices that enable users to access data through the network. They want to expand their technology-enabled business activities by capitalizing on cloud computing and mobility, but here again, security becomes a major issue: **48% of small businesses view "ensuring that security is not compromised" as the single biggest inhibitor to accelerating cloud use, and 42% of SBs report that when they build mobility plans, they are "most concerned about general malware infection on mobile devices."**

In all cases, complexity arises from the fact that security issues don't fall into a single category – there are a number of 'threat vectors' that apply to each layer of an SB's IT (and business) infrastructure. SB management worries about malware attacks on PCs that can cripple productivity and damage data; they are also concerned about the potential for identity theft, network intrusions and lost or stolen devices that can compromise customer privacy or open the door to fraud. SBs who embrace cloud computing as a means of enhancing service levels worry about the security of data housed by suppliers, and about potential breaches that may occur when communicating to these remote hosts.

Research shows that SBs are likely to identify multiple "biggest security concerns" that have a negative impact on the use of technology that is needed by their businesses. And there is good cause for this concern: **64% of small and medium businesses report that they have had one or more mobility-related security breach.**



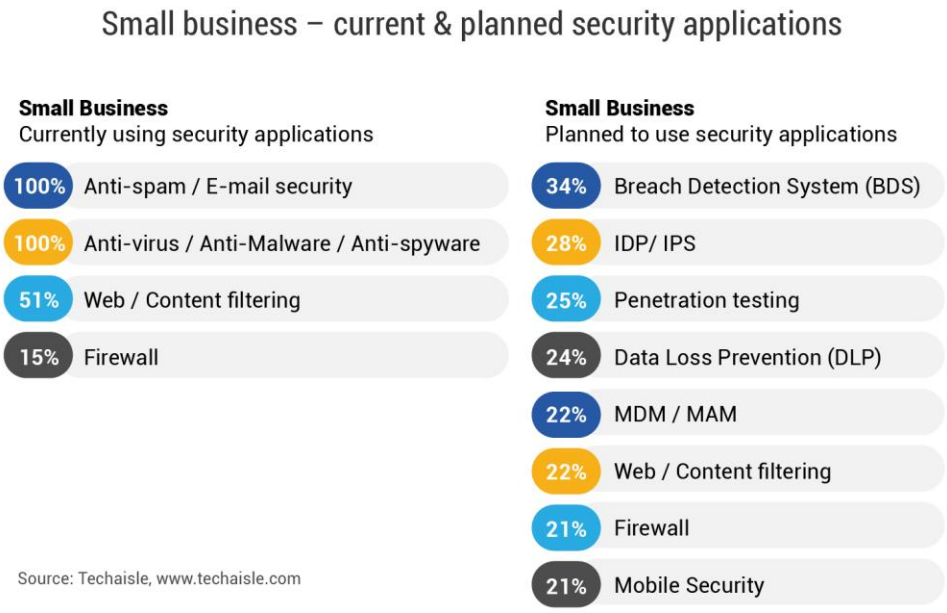


Raising the Shields

Faced with the dizzying variety of threats, SBs have developed an investment approach that aligns scarce resources with the areas of greatest exposure – and a healthy appetite for expanding defense resources over time.

Techaisle's survey of small businesses identified two security technologies that are universally deployed: anti-spam/email security and anti-virus/anti-malware/anti-spyware solutions. In both cases, SB management is protecting users and devices (and by extension, the customers served by those users) from the threats that are most likely to reach workers who rely on technology, especially those who – like everyone in a small business – 'wear many hats;' people who need to react to requests and opportunities as they arise, and who don't follow a tightly-defined daily routine. About half of small businesses have also deployed web/content filtering technologies, to establish an additional layer of protection against threats hidden on the Internet.

Data from the survey shows that small businesses are planning to deploy additional security 'shields' within the next year. These include breach detection systems, intrusion detection and prevention systems (IDP/IDS) and penetration testing that will help protect against targeted attacks, data loss prevention and mobile device management/mobile access management (MDM/MAM) solutions that keep data from leaking out of the business through smartphones, memory sticks and other portable devices, and other technologies designed to defend users and data – and the business as a whole.



Attack surfaces and threat vectors

Faced with so many urgent priorities, it can be difficult for an SB to stay focused on expanding its IT security 'shields.' When is enough, enough?

It's a fair question, but the answer isn't found in the spending allocated to cybersecurity. Instead, it's an issue of supply and demand.

If an organization used a single application – say, email – it would need a simple set of security products: anti-spam/email security, and perhaps an anti-malware suite to deal with problems that might arise when a user clicked on an attachment. An organization that had a slightly more expansive set of applications and data running on mobile, web-connected devices – say, users who created and delivered corporate documents and presentations, and worked on budget spreadsheets from remote locations – would need just a modest expansion to their security infrastructure – perhaps adding MDM/MAM and DLP systems.

However, small businesses want to take advantage of advanced technologies. They want to use collaboration to drive better productivity and increased contact with customers and prospects. They want to use cloud-based systems to access customer relationship management systems, advanced accounting applications and dozens of other solutions that enable SBs to look like – and compete with – larger organizations.

Each new use of technology increases business capabilities in a meaningful way. But it also increases the attack surface of the business – the number of ways that an SB is exposed to security treats. And because attackers are resourceful and creative (if malicious!), each new surface, along with each new breakthrough on the 'dark side' of technology, increases the threat vectors, or possible avenues of attack, that an SB must defend against.

Take cloud computing as an example. Cloud offers SBs he ability to access compute power and applications that were previously available only to much larger organizations. Cloud is unquestionably a major business resource for SBs; Techaisle research has shown that it is the most important element in SB technology strategies tuned towards building agility and competitive advantage. But cloud adds to the attack surface, opening new vectors that can be exploited by cybercriminals. SBs who commit to the cloud need to consider adding data and network encryption and other security practices and technologies to their existing, PC and data-focused security technologies, in order to ensure that they aren't harmed by their use of cloud as a business enablement tool.

Best options for small business productivity: mastering 'the transition game'

The maxim "the best defense is a good offense" is familiar to most of us: it has been quoted by military and political strategists, in legal and business circles, and in virtually every sports context. Sports is an especially instructive source for analogy, since in many, including basketball, soccer and hockey, there is also emphasis on the 'transition game' – the point at which defense morphs into offense, and a team is able to make headway towards scoring, rather than simply defending its own position.

> "Offensive operations, often times, is the surest, if not the only (in some cases) means of defense"
> – George Washington

In today's business environment, IT security presents a twist on these statements – one that provides SBs with guidance on how to align security capabilities with business growth.

Let's start with "the best defense is a good offense," a phrase that is attributed to General George Washington, Coach Vince Lombardi and dozens of others. Some might look at the attack vectors detailed above and say that with respect to IT security, 'defense is essential to survival' – but this mindset positions security strictly as a defensive measure, and results in security being positioned as a cost that can't be avoided but might be minimized. In a world where technology is a critical contributor to productivity, growth and profitability, though, security is not simply an expense. Capable 'shields' enable small businesses to deploy technology confidently, focusing on growth opportunities rather than threats.

> To be successful at any level, players need to manage transitions in a game
> – USA Basketball

This theme is even clearer when we focus on the concept of transition – of moving forward to press home capitalize on advantages as they arise. Businesses that view security strictly as a 'necessary evil' will find that security is an impediment to rapid change, as new systems are delayed by the need to 'bolt on' security as a final step before deployment. It is far better for SBs to establish a robust, flexible IT security infrastructure, one that is capable of supporting new functions as they are brought on line. SBs that view Cyber-defense as a core component of business-critical IT infrastructure can position IT security as a high-value, strategic activity, rather than as an 'anchor' or cost of doing business – they can be both safe *and* empowered.

Source: Techaisle, www.techaisle.com

The straight line

In small business, the best approach to new technology is almost always a straight line: a direct connection that links business drivers, a well-defined solution and a target outcome, and which includes selection guidance that SB executives can use to avoid mis-steps in the journey.

IT security meets this straight-line definition. The driver – a compulsion to deploy technology to increase productivity, growth and profitability while avoiding the perils of IT security breaches – are clear to anyone who is responsible for a small business. The solutions, which involve creation of 'shields' that protect assets ranging from networks and devices to users, data and customer trust, are based on proven technologies that are continuously updated research by an active supply community, can be understood in terms of established risk sources and responses. The guidance, which focuses on positioning cybersecurity as a growth attribute rather than a 'necessary evil,' helps SBs to avoid a security strategy that both increases risk and reduces new business potential. And the target outcome, use of technology to build an agile SB that can react quickly to new opportunities, describes a position that every SB would like to attain.

Small businesses have many challenges and limited resources. An approach to IT security that moves beyond 'safe' to 'empowered' gives SB executives an opportunity to reap real, tangible agility benefits that differentiate their organizations, covering both the requirement to safeguard assets and relationships and the potential to establish a platform for ongoing success.

About Techaisle

Techaisle is a global SMB IT Market Research and Industry Analyst organization. Techaisle was founded on the premise that Go-to-Market strategies require insightful research, flexible data, and deeper analysis. Understanding the value of data consistency across markets to inform strategic planning, Techaisle has remained holistic in its approach to Insights and provides globally consistent SMB and Channels analysis across geographies. To achieve its objectives Techaisle conducts surveys with SMBs and channels to understand market trends, opportunities, buying behavior, purchase intent, and IT priorities. Besides covering emerging technologies such as SMB cloud computing, managed services, mobility, social media usage, virtualization, business intelligence, big data, collaboration, networking its channel research coverage provides in-depth understanding of resellers and channel partners globally. Techaisle's insights are built on a strong data-driven foundation and its analysts are conversant with both primary research and industry knowledge, which is a rare combination. Techaisle offers its clients: Syndicated Research, Custom Primary Research, Consulting Engagement, Competitive Intelligence, and Segmentation. For more information, visit www.techaisle.com

Contact:
Ph: 408-4597751
5053 Doyle Rd, Suite 105, San Jose, CA 95129
www.techaisle.com

| US
| Singapore
| India

techaisle
www.techaisle.com
Global Industry Analyst & Market Research Orgnization
SMB Data You Can Rely On — Analysis You Can Act Upon