A TECHAISLE WHITE PAPER

Cyber Security:

Defending your digital business

Your business relies on its technology – but lurking around the corner are intruders who can disrupt or devalue your operations. This report shines a light on the sources of the problem, and how you can establish the control you need to get the best from IT

techaisle
www.techaisle.com

Cyber Security: Defending your digital business

Your business relies on its technology – but lurking around the corner are intruders who can disrupt or devalue your operations. This report shines a light on the sources of the problem, and how you can establish the control you need to get the best from IT.

Setting the stage: the link between business achievement and cyber security

In every corner of the globe, businesses are building new capabilities that rely on technology. Small businesses are automating previously-manual processes and digitizing key tasks and information sources. At the same time, large enterprises are dedicating vast resources to analytics and to digital transformation – capitalizing on the reach and opportunities enabled by digitalized processes.

Positioned – sometimes, 'squeezed' – between the agile small businesses and deep-pocketed enterprises are midmarket businesses: firms with 100-499 employees. These firms are striving to both stay ahead of smaller firms and to compete with global giants.

Figure 1. Top 10 midmarket business issues

Source: Techaisle global survey of 2075 midmarket (100-499 employees) businesses

As Figure 1 shows, midmarket executives are looking to drive better performance throughout their businesses. They are focused on quality and productivity improvement, measures that increase growth and profitability, and cost management and control-related issues.

Each of the ten issues identified in Figure 1 has a common thread: it is impossible to achieve without a highly-capable IT/business infrastructure. Midmarket executives know this: **97%** report that technology is either "very important" or "somewhat important" to their businesses, and **43%** report that they have become *more dependent on technology in the last 12 months*.

There is an important capability gap hidden in these statistics, though. Generally, these firms have relatively-small IT staffs (an average of 6.4 employees) that are tasked with keeping pace with the digital innovations of global leaders – delivering the IT-enabled services that customers have come to expect. They maintain corporate environments that include, in nearly all cases, a mix of cloud-based and corporately-owned infrastructure, supporting an unruly mix of corporate and employee-owned desktop, laptop, tablet and smartphone devices.

There is another, uncomfortable truth hidden in these statistics. As midmarket businesses become more dependent on technology – as they stretch finite resources to keep pace with global competitors – their businesses become more vulnerable to cyber threats. 'Security breach' isn't simply an abstract concept: it describes a scenario in which sensitive data is leaked, IT is forced to react to cloaked predators who might be based anywhere but have gained access to the inner workings of the business, workers are less productive, and the business as a whole risk losing the trust of its customers.

Identifying the threats

Which threats loom largest in the midmarket? A global research study of 2075 midmarket firms conducted by Techaisle found that some of the most popular midmarket solution areas – cloud and mobility – are also the source of some of the most serious threats to IT security in midmarket businesses.

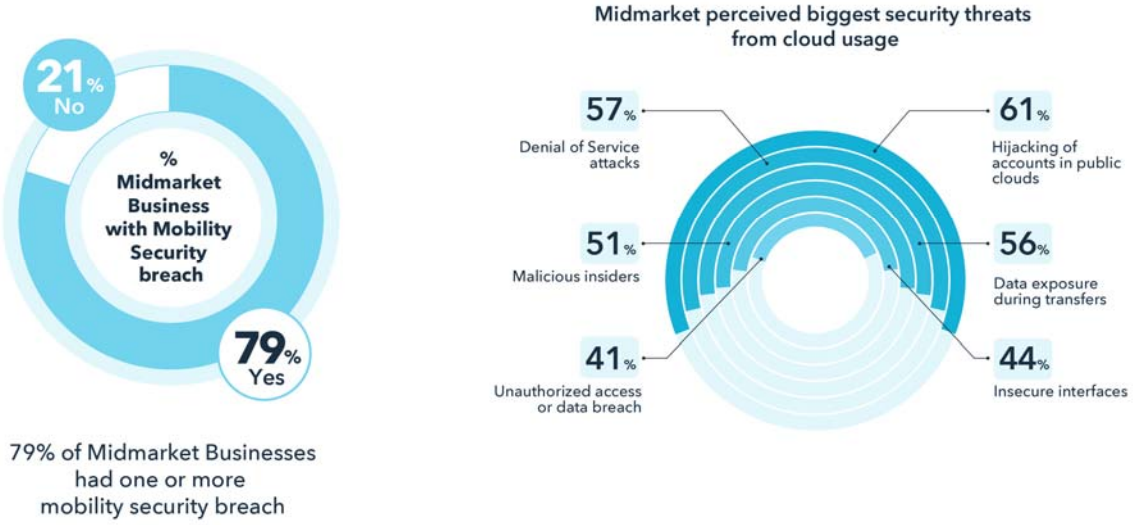
Figure 2 combines data on these two solution areas. On the left side of the Figure, we see that 79% of midmarket businesses *know* that they have had one or more security breaches resulting from mobility; experience suggests that the real number may be even higher, as some breaches can go undetected for months or even years.

Mobility delivers substantial, tangible benefit to midmarket firms: it allows on-the-go or remote workers to be highly productive, working more closely with clients, delivering service from field locations, or extending their work options to facilitate better work/life balance. But as the Figure shows, mobility also increases the potential for security breaches. Lost or stolen devices, insecure logins from remote WiFi locations and other device or connection security issues represents a cost – in data loss, regulatory or audit exposure, or lost worker and/or IT productivity – that midmarket firms need to account for, in the form of better IT security or possible loss of customer or regulator confidence.

Cloud computing is also a boon to midmarket business efficiency – and at the same time, a potential source of IT security exposure. Along with analytics, cloud is seen by midmarket firms as one of the

technologies with the greatest potential for enabling digital transformation over the next five years. But as Figure 2 illustrates, cloud is also seen as expanding the threat profile of midmarket businesses. More than 60% of midmarket respondents report that they are concerned by the prospect of having user accounts hijacked in the cloud; more than half worry about denial of service (DOS) attacks, the potential for data loss during transfers between corporate and cloud-based system, and even leaks from staff members or contractors looking to use cloud as a means of exfiltrating data. As is the case with mobility, to capitalize on cloud benefits, midmarket organizations need to invest in the tools needed to mitigate IT security threats.

Figure 2. IT security threats: mobility and cloud



Source: Techaisle global survey of 2075 midmarket (100-499 employees) businesses

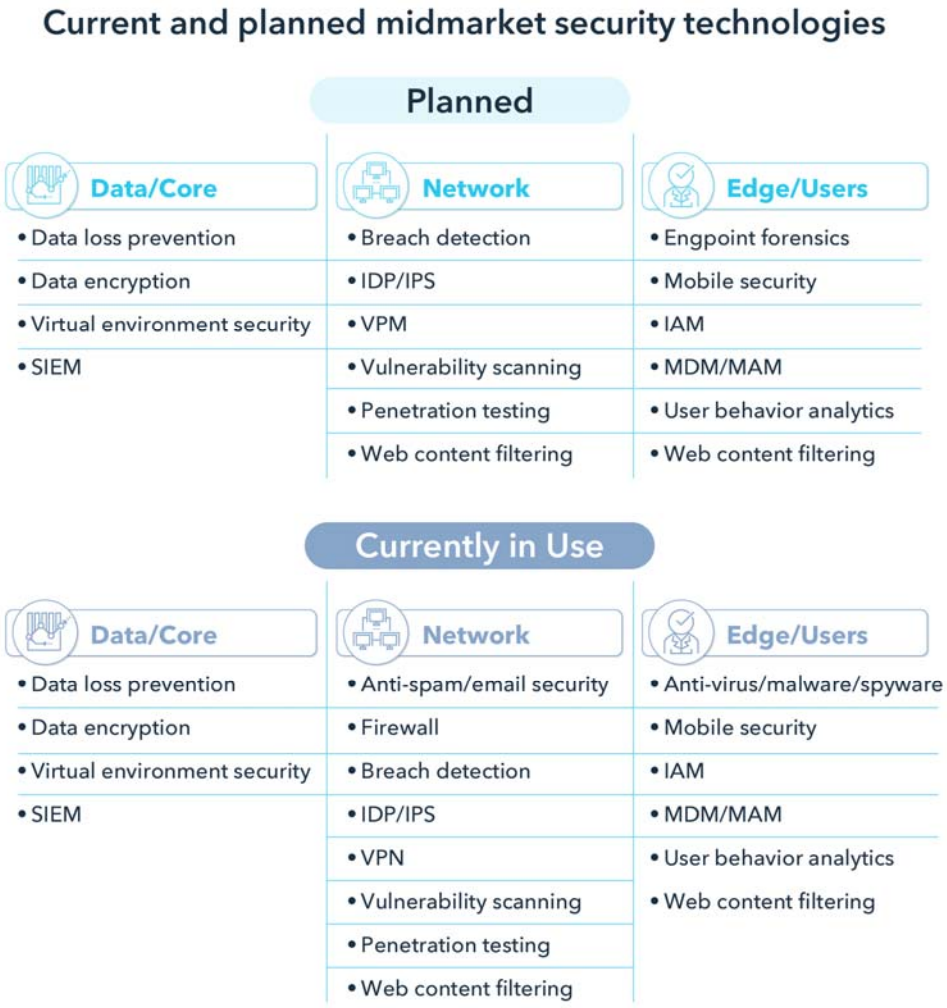
Shields up! Investing in security solutions

With exposure attaching to the solutions that deliver greatest benefit to midmarket companies, it's not at all surprising to find that a clear majority of midmarket firms are already allocating resources to IT security, and that further investment is planned over the next 1-3 years, with 60% planning increased allocations to IT security, and overall security spending by midmarket businesses poised to increase by 8% annually.

Figure 3 provides an intriguing view of midmarket IT security 'shields' and plans. The green box at the bottom of the figure details the technologies that have been deployed by at least some of the midmarket firms surveyed by Techaisle. As the Figure indicates, midmarket firms are investing in security solutions that protect users and edge devices; an even richer portfolio of network-centric security offerings; and are also deploying solutions that protect data and core physical (and virtual) assets. The blue box at the top of the Figure enumerates the technologies that midmarket businesses are planning to invest in in the

future. It's interesting to note that, apart from technologies that are ubiquitous (anti-spam, firewalls), midmarket firms are investing in the technologies that are already present in the environment, indicating a commitment to deepening the resources that they use to combat cyber threats. This provides an important insight: security is not a 'set it and forget it' proposition; security technologies need to be continuously updated to keep pace with expanding external threats, as well as with changes to business-wide and individual user threat profiles.

Figure 3. Current and planned midmarket security technologies



This panoply of security technologies offers the promise of protection – but are midmarket firms able to effectively manage multiple 'shields' to deliver comprehensive defense against threats? Techaisle research indicates that on average, midmarket firms have **6.4 IT employees** – staff that is responsible for managing the IT budget, procuring, configuring and deploying physical assets, supporting users, patch management…and researching, acquiring, aligning and continuously updating security technologies.

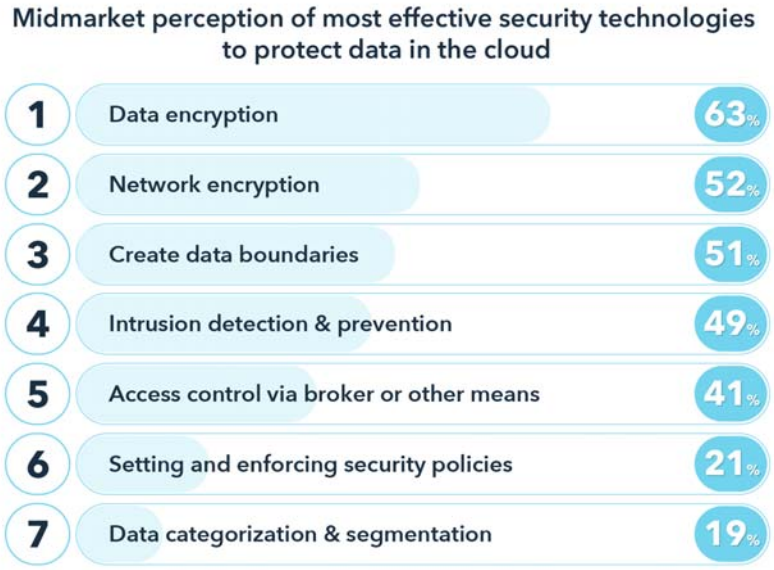
Midmarket firms are adept at stretching scarce resources to cover extensive requirements, but they will likely need external assistance in keeping pace with the changing security landscape.

Where should midmarket firms focus first?

To help provide guidance, Techaisle asked respondents to identify the security approaches that they consider to be most effective in protecting their midmarket businesses against cyber threats – and at the same time, protecting the business against loss of customer trust and brand damage. The results from this question, shown in Figure 4, demonstrate that IT organizations need to combine technology with effective data and security management practices:

- The top two responses focus on encryption: ***data*** encryption, which applies both to data that is 'in motion' across the public network and 'at rest' on servers or client devices, and ***network*** encryption, which is especially important in supporting cloud and mobility
- The fourth and fifth highest-ranked items, ***intrusion detection and protection*** and ***access control*** are technology solutions that help to defend against cyber attackers.

Figure 4. Most effective IT security options for midmarket



Source: Techaisle global survey of 2075 midmarket (100-499 employees) businesses

- The other three items on the list – ***creating data boundaries***, ***setting and enforcing security policies*** and ***data categorization and segmentation*** – represent actions that can (and should) be taken internally. Each of these measures is an important ingredient in the overall cyber defense of the business, but each demand that the midmarket business allocates scarce resources to security management.

WIFM? Cyber security in real-world contexts

The many challenges associated with cyber security make this a daunting challenge for both executives and IT staff working in midmarket businesses. Many might be tempted to wonder whether extensive focus on (and investment in) cyber security is really a wise use of resources that are in demand across the organization.

The reality, unfortunately, is that experts believe that a data breach is a matter of 'when' not 'if.' Every midmarket business is a potential victim of cyber intrusion – and every responsible executive and IT management team will need to deploy technologies and develop strategies to protect against intruders – detect the presence of hackers who have gained access to corporate data – protect data 'in motion' and 'at rest' via encryption, to prevent exfiltration of critical, sensitive information – and to react to breaches when they are discovered.

Figure 5. Defending your business against cyber threats

Source: Based on the NIST cybersecurity framework

Effective cyber security isn't simply a matter of good governance – it's also a critical aspect of ensuring that staff members are able to be effective and productive. Virtually all midmarket businesses have front-line staff who may be targets of cyber-predators: ***Desk-centric workers*** who spend an average of more than four hours per day on a desktop computer, ***remote workers*** who access and write to corporate systems from a nearly-infinite variety of remote locations, '***on-the-go pros***' who juggle multiple devices

that each fill a specific business need, plus engineers, creative professionals and others whose link to technology is critical to their work.

Regardless of role or work pattern, each connected worker is vulnerable to cyber attacks, and each requires effective protection. Some of the key considerations for midmarket security strategists include:

- ***Defense against phishing and malware***: It's tempting to consider these types of attacks to be random and infrequent, but research conducted by Dell has shown that 36% of staff members will open emails from unknown senders while at work, and that 72% of employees would share sensitive, confidential or regulated company information under certain circumstances – generally, in pursuit of better collaboration and/or increased productivity. An effective approach to phishing and malware defense, combining endpoint and network technologies with policies and training, helps to ensure that your most proactive workers aren't also potential targets for intruders.
- ***Mobile device (and data, and user) protection***: For many organizations, mobility is a central attribute of efficiency: Techaisle research finds that midmarket firms see mobility as a means of boosting productivity, improving customer service and supporting new, flexible work patterns demanded by employees. Midmarket businesses want to capitalize on these benefits – but there's a requirement to defend against exposure as well. Midmarket firms that need to align mobility benefits with security requirements invest in technologies like mobile device management and mobile access management (MDM/MAM) solutions.
- ***The need for encryption***: Good data security via encryption helps to ensure that users who are looking to accelerate decisions and outcomes don't inadvertently expose confidential information. Data protection via encryption is essential for businesses that have information in the cloud, that have workers in remote locations, that have websites that could be targeted by hackers…in short for midmarket firms of all descriptions.

Addressing real-world challenges

There is a conundrum contained in the examples above. Most midmarket businesses would recognize that desk-centric workers, remote workers and on-the-go pros are important to their success, and most would agree that taking the steps needed to safeguard these users, their data and devices and the connections that they open into the corporate environment are also important to the health of their organizations. However, the Dell research cited above found that 76% of employees believe that their companies "prioritize security at the expense of employee productivity;" just 36% "feel very confident in their knowledge of how to protect sensitive company information." IT needs to balance the productivity of key staff with the corporate requirement for cyber security, while recognizing that both objectives are essential to business viability.

Concluding guidance

There is no simple template for defending a digital midmarket enterprise. Each of the options shown in Figure 4, each of the technologies listed in Figure 3 and each of the strategies discussed elsewhere in this report are important to delivering the cyber security needed to support the business activities of midmarket employees and their organizations. Cyber threats are real, and are growing in scope, sophistication and impact; despite limitations in staff resources, midmarket businesses need to develop and continually update their cyber security postures. Ultimately, this is a complex issue that has no defined horizon. To stay competitive in the digital world, midmarket businesses need to capitalize on the technologies, practices and supplier insights delivered by trusted advisors that allow them to provide a safe environment that serves staff, shareholders and customers.

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