KASPERSKY lab

Business Attitudes Toward Cybersecurity 2014

Contents

The Main Findings

Current Status of Cybersecurity in Business

- All companies, regardless of their size, rarely use the maximum level of protection available to them
- When asked, 43% of very small businesses (VSBs) said that 'IT security' involves combating malware and 27% said that it involves ensuring the physical security of company data, whether on premise or on the road. However, for larger businesses the main challenge is the complexity of their IT security needs.
- Customer information is seen as the most critical type of data to protect in all regions (**25%**) except China, where payment information is the top concern (**28%**).

Business Cybersecurity Trends

- The adoption of BYOD among SMBs and Enterprises continues to grow.
- Employees are using company-managed smartphones more often (**64%**) than tablets (**36%**).
- Out of 100 respondents, 26 said that their business uses Virtual Desktop Infrastructure (VDI), but just nine apply Virtualization-aware anti-malware for virtual desktops.
- Those VSBs that employ IT specialists prefer to use a business solution (**71%**), rather than a home solution (**14%**) or free products (**14%**) for their IT security. If they are using free products, these tend to be selected by the VSB's owner (**22%**) or non-IT specialists (**28%**).
- When choosing between business and home solutions, VSBs prefer the simple, cheap way of getting basic but powerful AMS protection from home products.

Methodology

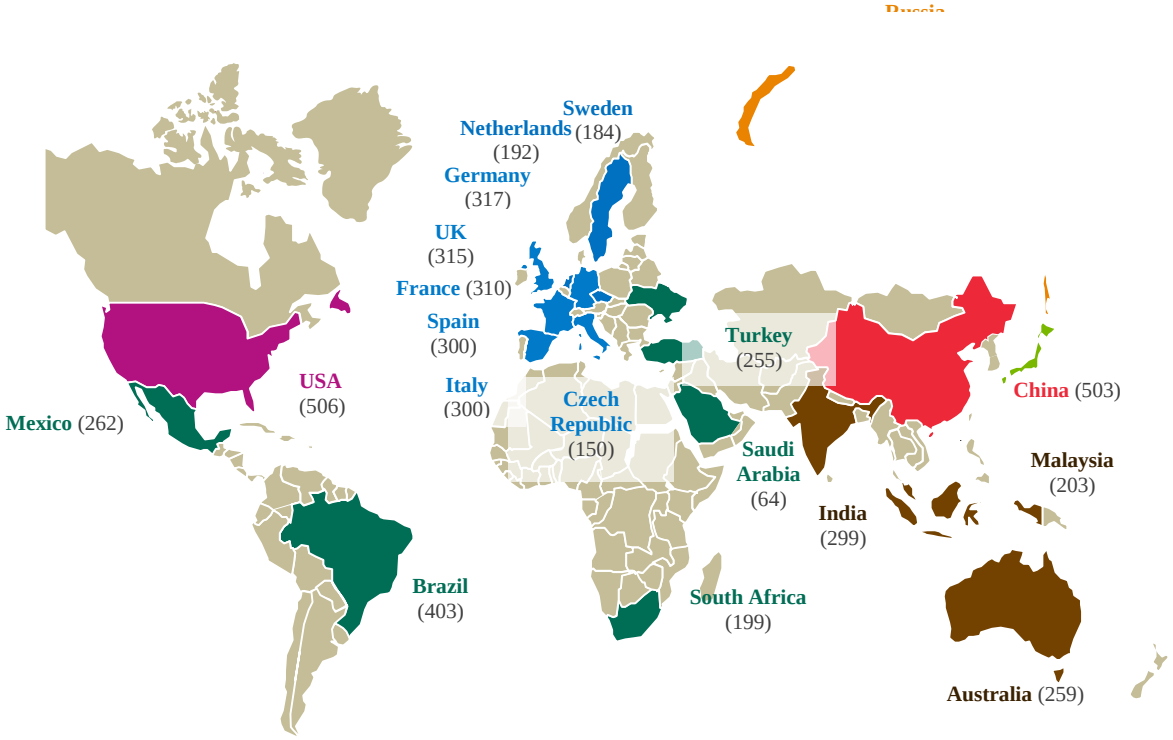

Figure 1. Geography of the research

A total of 6,219 respondents from 21 countries took part in this year's B2B Brand Tracking 2014. Respondents represented companies employing 1-1500+ people. All respondents were categorized according to the size of their business: Very Small Business (VSB, 1-50 employees), Small and Medium-sized Business (SMB, 50-1500 employees) or Enterprise (1500+ employees). The survey was conducted from October to November 2014.

All participants answered questions concerning the main obstacles they faced when building and maintaining a reliable IT infrastructure. Respondents also answered questions about the resources they use to learn about data protection and how they choose their IT solutions.

Current Status of Cybersecurity in Business

One of the objectives of the research was to understand whether businesses are ready to face modern cyberthreats. Respondents were asked about the security technologies deployed within their IT infrastructure. As expected, the businesses with high employee numbers take IT security most seriously. These businesses are also more willing to

implement advanced protection features. However, the answers show that even Enterprises do not always use the maximum level of protection available. Detailed figures on the use of technologies by businesses of different sizes can be found in Appendix A.

IT security consists of both organizational and technical measures. The respondents from businesses with more than 100 employees were therefore asked questions about employee commitment to IT security, as well as the importance of IT security throughout their organization.

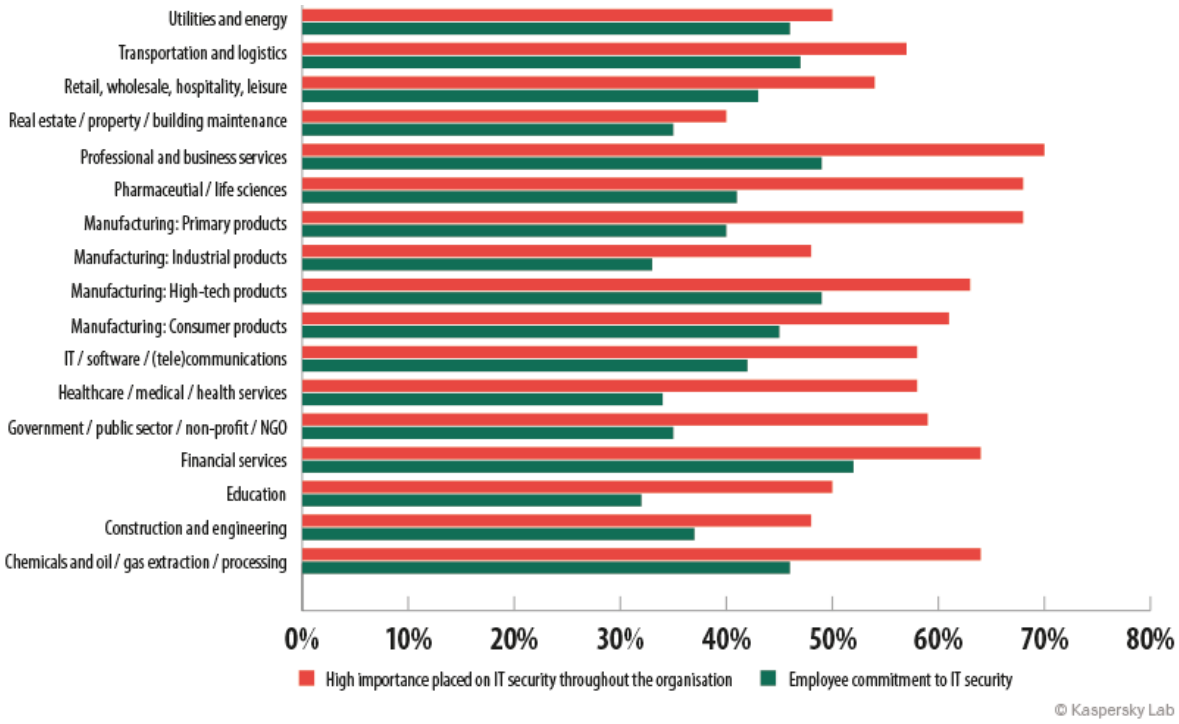

Figure 2. The importance of IT security and employee commitment (vertical layout)

42% of respondents said that employees are involved in IT security: their management layer takes part in developing and enforcing IT security goals and policies, Non-IT managers follow and enforce IT security rules and all other employees are generally cautious and responsible in their behavior.

58% of respondents said that their business places a high importance on IT security across the whole organization. Their internal rules obligate maintaining a high IT security level for customers and employees, and demanding a high level of IT security from suppliers, subcontractors and distributors. However, the vertical layout shows that even businesses in sensitive industry sectors - such as utilities and energy - do not always pay appropriate attention to IT security.

Depending on their size and sector, businesses identify different priorities for IT security.

For example, VSBs with fewer than 25 employees said it is a major priority for them to guard against external cyberthreats, such as malware (43%). This is because the number of cybercriminals is increasing as technology becomes increasingly cheap and simple-to-use. Nowadays, a teenager with basic computer programming knowledge can became a cybercriminal, stealing business data from a business's IT system just for fun, or to show off to peers.

27% highlighted the physical security of business-critical systems and 25% said the security of mobile/portable computing devices was a priority.

Bring Your Own Device (BYOD) strategies must also be considered in the context of IT security. Some VSB employees, store business data such as their clients' personal information, prices, business development plans and more on their own devices without any backup or mobile security protection. This makes the risk of financial loss even higher.

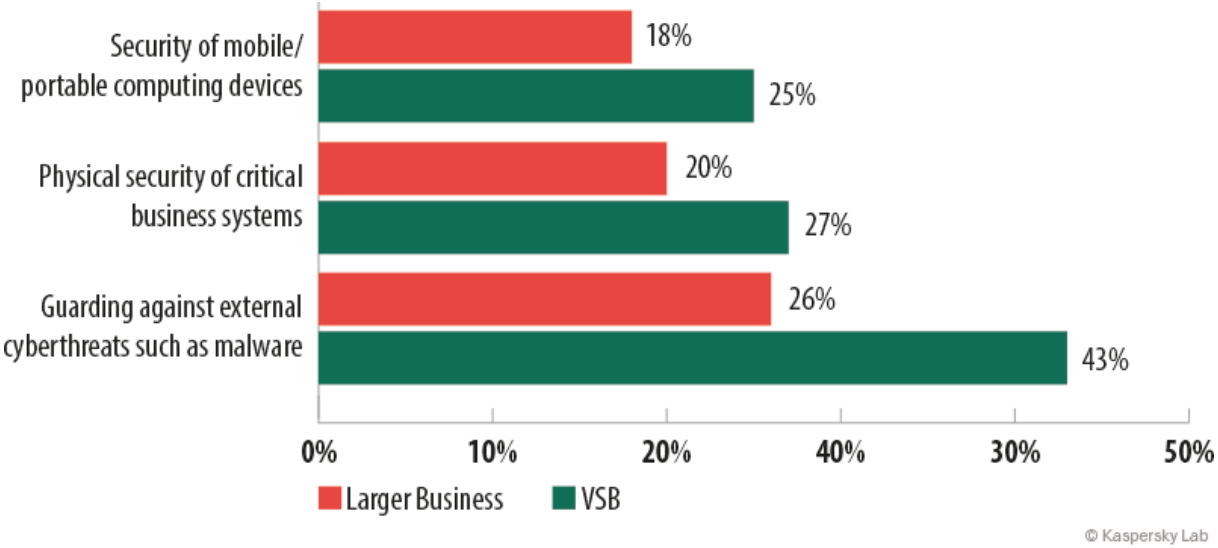

Figure 3. Cybersecurity priorities *for businesses of different sizes.*

It is important to emphasize that VSB priorities are greater when compared with those of larger businesses: 26%, 20% and 18% respectively. Four out of five representatives of SMBs and Enterprises noted that external threats such as cryptolockers or ransomware do not represent a serious threat to their businesses. Furthermore, more than two thirds of representatives of these groups accepted that BYOD trends present an increased IT security risk, but they do not consider the threat of corporate espionage through mobile devices as a serious concern.

The main challenge that SMBs and Enterprises face is the complexity of their IT security needs. As a result, the larger companies often use business solution bundles because they provide integrated protection for all PCs and devices within the corporate network. With a bundle, the business doesn't need to worry about buying and maintaining separate IT security solutions for different endpoints.

When it comes to protecting data against external threats (mobile device theft / loss; unfair competition; cybercriminal activity, etc.), the VSBs were largely in agreement about the types of information that should be protected first.

It is important for very small businesses to work closely with customers and to do everything they can to retain clients. All the VSBs questioned prioritized the safety of their customers' personal information (names, addresses, numbers, e-mail addresses, etc.) For VSBs, providing customers with the best service and keeping their details is key to securing loyalty. This was expressed by 25% of respondents in almost all regions, excluding China and North America, where there were different priorities (China – trade secrets (28%); North America - social security numbers/government-issued IDs (24%)).

Participants also prioritized the protection of payment information, such as customer credit card data (13%), while 12% prioritized trade secrets/intellectual property and another 12% said it's vital to protect the organization's financial information.

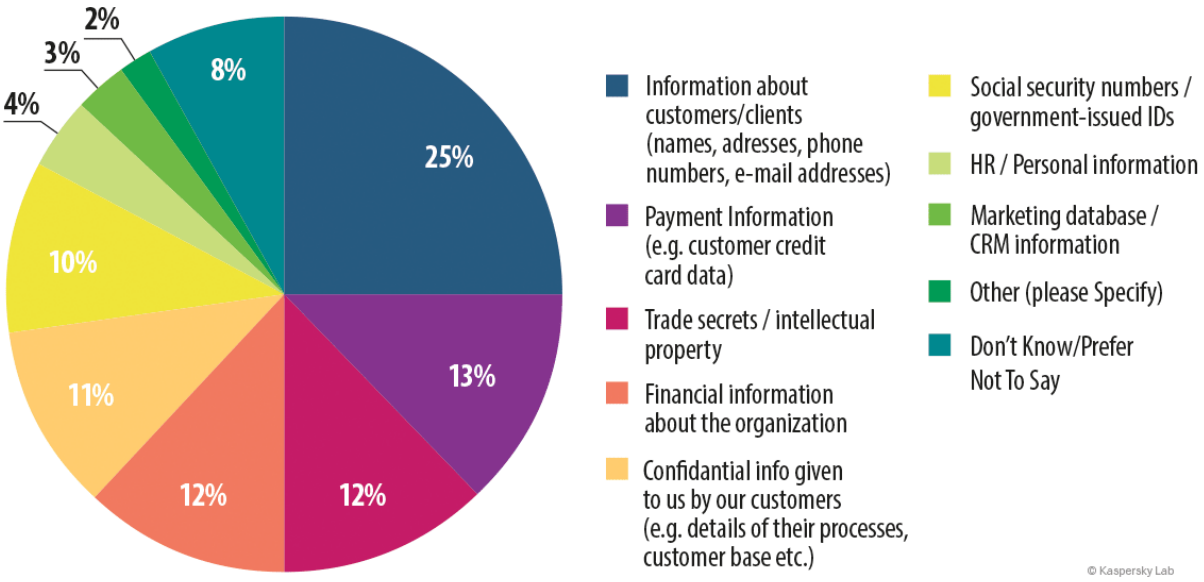

Figure 4. The types of information that are the top priority for IT security in VSBs

Business Cybersecurity Trends

BYOD

BYOD (Bring Your Own Device) is one of the most widespread trends today and sees employees using their personal devices (mobile phones, tablets and laptops) for business tasks.

The number of smartphones and tablets used by the SMB and Enterprise segments continues to grow. In 2012, the share of smartphones and tablets used by SMBs was **61%** and **41%** respectively. However, by 2014 this share had grown to **70%** and **57%** respectively. The same trend can be seen in Enterprises: use grew from **60%** (smartphones) and **43%** (tablets) in 2012 to **70%** and **59%** respectively in 2014.

Nowadays, it's not only the large businesses that are using employees' personal mobile devices as part of the corporate network. For some VSBs BYOD is an appropriate and useful business strategy. More than **62%** of VSBs noted that they use company-managed mobile devices, but these devices are predominantly smartphones (only **36%** are using tablets). This means that more than half of all respondents store different kinds of business information on their own smartphones - in the case of theft or loss this could be used against the company.

In fact, it is so common to use mobile devices at work today that only **32%** of VSBs agreed that a BYOD strategy presented an increased IT security risk to their business. **68%** of respondents saw no threats from using personal devices at work (compared to **58%** of larger businesses). Only **13%** of VSBs were interested in information about mobile device management and BYOD being included on anti-malware solution software developer

websites (compared to **18%** of larger businesses). These results confirm that most VSBs do not know or do not want to know how to manage mobile device security and do not think about how important it could be in terms of business growth and development.

Choosing and managing an IT security solution

According to respondents, businesses use various configurations of IT infrastructure: **68%** said they use physical servers, **52%** have implemented server virtualization technologies and **26%** have deployed Virtual Desktop Infrastructure (VDI). Majority of them still prefer to use their own hardware, while others entrust the allocation of servers to remote data centers, and server management to third party companies.

		Physical infrastructure	Server virtualization	Desktop virtualization
Use physical hardware installed ...	... on premise	70%	40%	49%
	... in data center	11%	30%	22%
	... on premise and in data center	19%	28%	28%
Who maintains the systems	Internal IT staff	66%	49%	59%
	Third party IT staff only	12%	21%	15%
	Internal and third party	22%	29%	26%

Table 1. Hardware allocation and approach to management

It is sometimes assumed that larger businesses have their own IT specialists to administer corporate servers. However, this is not always the case - some Enterprises delegate the management of servers to third parties, exposing their IT infrastructure to additional risks.

		Overall	VSB (1-50)	SB (51-250)	MB (251-1499)	Enterprise (1500+)
Servers used by the business	Physical servers (non-virtualized)	68%	54%	73%	72%	78%
	Virtualized servers	52%	25%	52%	71%	73%
	Virtual desktops (VDI)	26%	11%	22%	36%	39%
Servers at least partly managed internally	Physical servers (non-virtualized)	59%	42%	65%	66%	73%
	Virtualized servers	40%	15%	40%	58%	62%
	Either	22%	9%	19%	31%	34%

Table 2. The use of virtualization and allocation of equipment in businesses of different sizes

Not all companies have an IT department or even in-house IT specialists. That is why, according to the survey results, different types of decision-makers have a casting vote over the choice of security software at these businesses.

The most popular finding here is that owners (**49%**) and non-IT managers (**45%**) are in charge of choosing the security software at companies with 1-10 employees, while only **6%** of these companies rely on IT specialists.

Respondents from businesses with 11-25 employees said that they trust the choice of security software to non-IT managers (**50%**), while owners (**24%**) and IT specialists (**26%**) have less influence.

Respondents from businesses with 26-50 employees stressed that they have at least one IT specialist who is responsible for choosing security software (**37%**), with non-IT managers and owners taking second and third places with **36%** and **26%** respectively.

Companies with up to 100 employees provided unexpected results here. About **55%** of these respondents said they have a specialized internal IT department or at least one IT specialist.

At the same time **22%** of respondents said their security software is managed by non-IT specialist managers. Furthermore, **13%** of respondents confirm that security software within the company is administered by employees themselves, while only **16%** of VSBs use any third party services (such as outsourced IT consultants). It is clear that companies are exposing themselves to danger by trusting the management of IT to non-IT specialists. Many respondents state that because they have a very small business, there is no need to have an internal IT specialist. However, this could lead to an increasing number of vulnerabilities in the corporate IT system.

With different decision-makers we can see varying patterns in the selection of IT security products. Business solutions, for example, are less likely to be selected by non-IT specialist management. **71%** of IT specialists prefer to use a business solution rather than a free (**14%**) or home (**14%**) product. Free products are more likely to be used by non-IT managers (**28%**) and owners (**22%**). When the decision-makers speak about purchasing business solutions, it's likely that they are referring to bundles. Almost **49%** of respondents consider using IT security suites, with a number of different types of IT security software (such as anti-malware, anti-spyware, encryption, application control etc.) within their company in the next one to two years. However **31%** do not consider using bundled IT security solutions because they are too complex for their business needs. This compares to the **72%** of mid-sized businesses that selected bundles.

Despite this, it would be wrong to assume that free security solutions are restricted to VSBs. **6%** of small businesses, **3%** of medium-sized and even **3%** of Enterprises are still using free solutions.

Studying the last three years, we can see a shift in IT security priorities. Only two years ago, almost **83%** of VSBs were using business solutions to fix their own IT security needs. Nowadays, free (**21%**) and home (**10%**) products are more likely to be used while the use of business products has lowered (**68%**). The survey's participants share the misconception that today's free and home solutions are enough to keep customer data and business operations safe and secure.

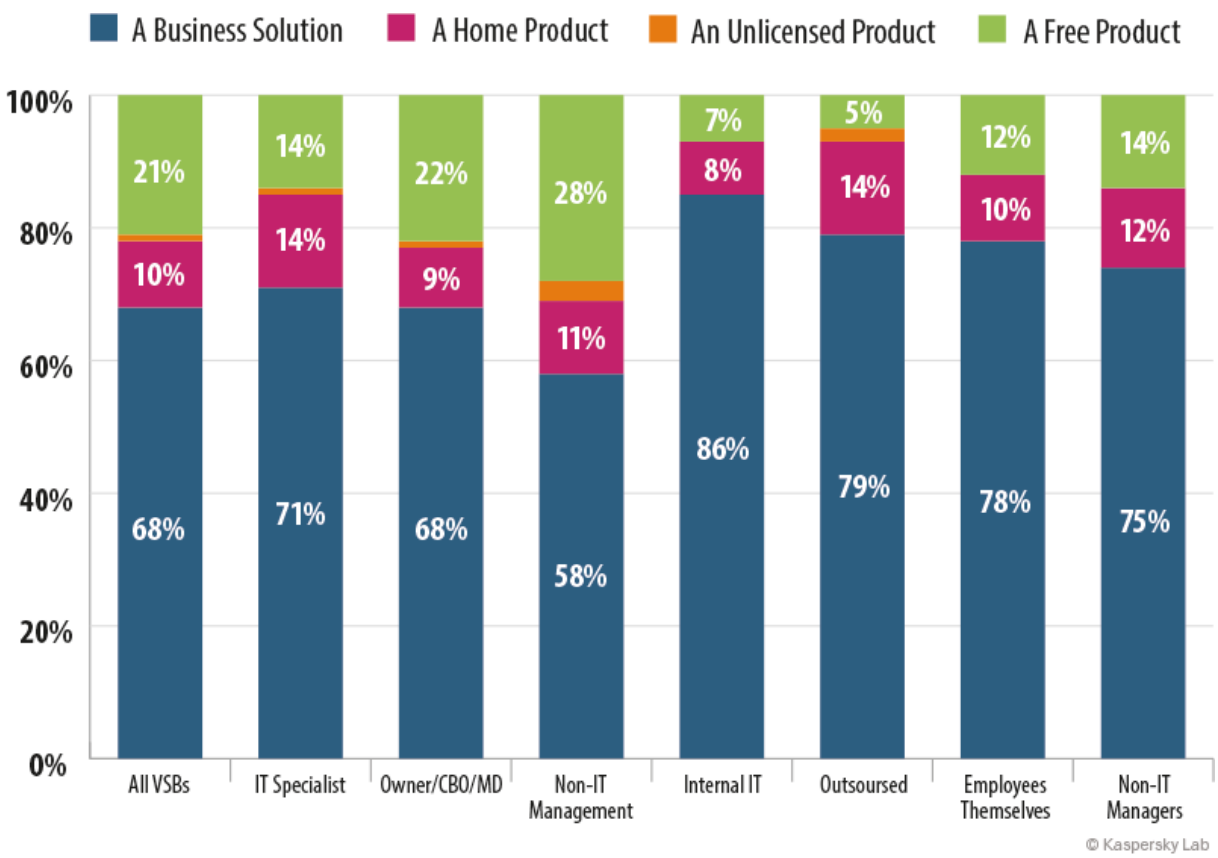

Figure 5. Priorities when choosing an IT security solution, by type of decision-maker

It is interesting that different regions have different solution preferences. The number of business solutions used are continuing to grow from **68%** to **73%** in North America, while in APAC, Japan, Russia, China and Western Europe it is much lower (**55% - 75%**) and falling. For example, the use of business solutions in APAC is down from **82%** to **63%,** while the use of home products has increased (from **4%** in 2012 to **23%** in 2014), and the share of free products has not changed. Japan bucks this trend. Here, free products have become much more popular with a percentage growth from **0** to **23**, while the share of business products has decreased (from **79%** to **56%**) and home products have become less popular (from **21%** to **19%**).

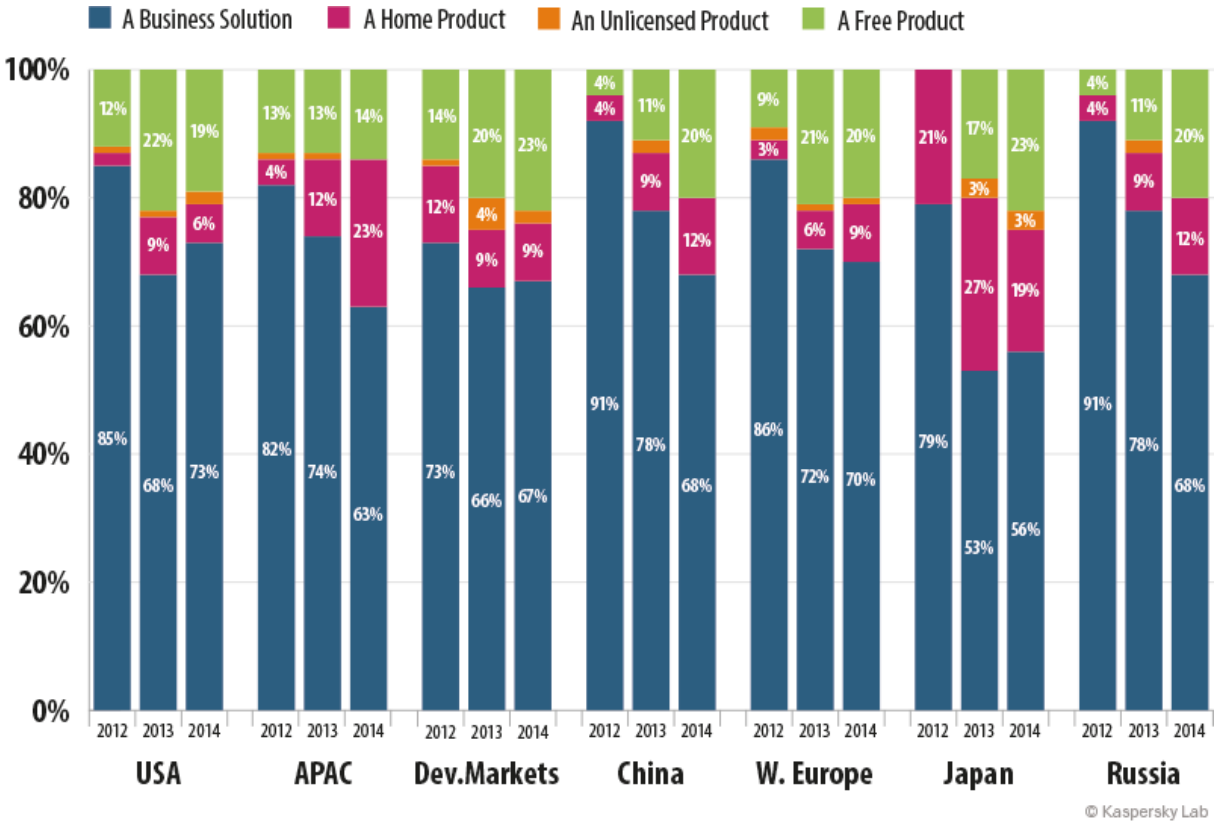

Figure 6. Priorities when choosing an IT security solution, by geography.

VSBs give several reasons for making their IT security solution choice. Home solutions offer them a simple and cheap way of getting basic but powerful anti-malware protection. On the other hand, free solutions are attractive to businesses where needs are simple and the perceived threat is low.

In India, many users of free products have upgraded to a paid-for home solution due to their desire for increased security. However, they were unwilling to pay for a more expensive and complicated business solution. This change is partly the result of a new trend in flexible business operations: offices have become remote and people are increasingly working with their own devices. There may therefore be no reason for a business to buy a complex and expensive solution if employees already have solutions at home. The employer simply needs to permit them to work at home and use home computers.

Figure 7. How VSBs chose security solutions - in their own words.

When selecting an IT security solution, a VSB prioritizes practicality (**27%**) and the need to keep things simple (**28%**). In addition, VSBs stressed that consistent performance (**31%**), responsiveness to business needs (**21%**) and security experts (**27%**) are important.

VSBs look at several elements when making their choice. They require a solution that has a suitable price point, is user friendly, transparent, jargon-free, flexible and easy-to-work with.

A solution that offers “good protection at a reasonable price” is the most popular selection. However, this requirement is dropping year-on-year. Instead, “the cheapest possible solution” is gaining popularity (from **5%** to **44%**) in almost all regions, particularly in China, APAC, Japan and North America.

Conclusions and Recommendations

The survey brought to light one contradiction. On the one hand, most businesses with less than 25 employees do not have an internal IT specialist. The IT security solutions are managed by non-IT specialists instead. On the other hand, all of these businesses understand the importance of securing customer data and business operational information.

VSBs require a reliable IT security solution that is suitable for their business needs but they do not want to spend a lot of money on it. In fact, a free solution is ideal. This strategy comes with a risk - selecting a solution based on cost, or relying on a free solution gives the business little or no guarantee of reliability or technical support. It might not be up-to-date or able to protect against the latest threats.

It’s important for each business to find the right balance of needs and capabilities. Sometimes it is better to spend a little more money in order to get the peace of mind that your business is in safe hands. Nowadays it is possible to purchase an easy-to-use IT security solution that provides reliable protection at an attractive price.

The results also show that all companies, even Enterprises, rarely use the maximum level of protection available to them. For example, only **14%** of VSBs, **27%** of medium-sized businesses and **31%** of Enterprises use a Mobile Device Management solution to protect and control employee devices in the corporate network. This is worrying as the popularity of BYOD continues to rise.

Currently there are no obstacles to using mobile devices at work. In some cases it is more practical to solve a business task with a mobile device, particularly if that task needs to be done immediately and the employee is out of the office. At the same time, businesses need to be aware that cybercrime using lost or stolen devices continues to increase. With that in mind, it is important that businesses protect all devices within the company’s network from cybercriminals.

Last but not least, the results bring decision-making to life. They show that it’s often the non-IT managers within a business who decide on the IT security solution. These managers do not have the relevant knowledge to select a solution appropriate for their company’s needs or to manage it effectively. Therefore, it’s vital that suppliers work proactively to educate customers and help them make the right choice.

Appendix A

% Organisations with technology implemented ccross the whole organisation	Overall	VSB	SB	MB	Ent
Endpoint-based URL filtering / website blocking	33%	21%	35%	37%	47%
Endpoint network access control	31%	19%	31%	38%	42%
Endpoint data loss prevention	29%	20%	29%	35%	35%
Endpoint application control	28%	17%	29%	31%	41%
Endpoint port and device control	27%	16%	26%	29%	40%
Endpoint encryption	27%	16%	26%	33%	40%
Anti-malware agent for mobile devices	26%	20%	24%	32%	32%
NET: Any advanced endpoint functions fully implemented	**57%**	**41%**	**59%**	**66%**	**71%**
Client management / systems management	26%	14%	25%	31%	38%
Mobile device management / control (MDM)	21%	12%	21%	27%	31%
NET: Any management functions fully implemented	**31%**	**17%**	**31%**	**39%**	**43%**
Server-based anti-virus / anti-spyware	38%	23%	44%	45%	50%
Data Loss Prevention (DLP) for Exchange	20%	8%	20%	26%	32%
Data Loss Prevention (DLP) for SharePoint	14%	4%	10%	21%	24%
NET: Any server-based functions fully implemented	**42%**	**24%**	**48%**	**52%**	**56%**
Virtualization-aware anti-malware for virtual servers	17%	6%	15%	26%	27%
Virtualization-aware anti-malware for virtual desktops (VDI)	9%	3%	6%	14%	14%
NET: Any anti-malware fully implemented on virtual infrastructure	**20%**	**7%**	**17%**	**31%**	**31%**

Table 3. Use of technologies by companies of different sizes.