Exclusive 2013
Survey Results

IT Security. Fighting the silent threat.

A global report into business attitudes and opinions on IT security.

Contents

About the survey

Why read this report?

- **Gain a global perspective on the state of IT security in business today**
- **Find out what other companies are thinking, planning and doing**
- **Benchmark your organisation against your peers**
- **Gain access to expert analysis from Kaspersky Lab researchers**

Kaspersky Lab's Global IT Risks survey, conducted by research consultancy B2B International, is now in its third year. This survey speaks to IT professionals across the world, looking to understand their attitudes, opinions and beliefs about IT security and its impact on their organisation. By doing this, we hope to establish a global benchmark for the industry, to help businesses of all sizes and types gain a broader perspective of IT security thinking.

Executive summary

The average cost of an IT security breach is $50,000 for an SMB and $649,000 for enterprises

The survey in summary:

- **2,895 interviews**
- **24 countries**
- **All IT professionals working in organisations with at least 100 seats**
- **All with 'good working knowledge' of IT security issues**

This year's Global IT Risk Survey contains two new aspects. Firstly, we segmented the data into SMB organisations (10-1,500 seats) and enterprise organisations (1,500+ seats). While many of the results are closely aligned, there are some interesting areas of divergence, which this report details. Certainly one that stands out is a worrying lack of IT security knowledge and understanding in smaller businesses.

The second new aspect was to get our respondents to quantify the financial damage that an IT security breach caused. For more details see Chapter 5. The average numbers equate to $50,000 for SMBs and $649,000 for Enterprises. Essentially, this shows that IT security breaches are proportionately far more damaging for SMBs than large enterprises.

The rest of the survey follows the topics we've tracked in previous years. It is always interesting to see changes and this year the survey contains some surprising and, at first glance, contradictory results.

On one hand, once again the top two concerns for IT professionals were 'preventing IT security breaches' – 34% up from 30% last year; and 'data protection' – 28% up from 26% last year. However, the vast majority of respondents under-estimated the volume of malware and there was a 6% drop in those who say they have seen an increase in cyber-attacks.

Is this cause for complacency? Our analysis suggests that is it not that simple. But largely, businesses are to be credited for investing in new tools to protect their businesses, and in recognising the importance of IT security.

The challenge ahead is that IT security problems used to be more 'noticeable' than they are now. Malware caused obvious system issues, which were highlighted and fixed. Now, malware has become a lot more sophisticated. No longer the realm of bedroom hackers, threats to businesses today are engineered by professional criminals intent on stealing and using valuable data – either for direct financial gain (accessing bank accounts, for example) or to sell on the very large open market for personal information.

This is borne about by one of the most concerning statistics revealed in the report – that 35% of surveyed organisations have lost business data as a result of external IT threats.

This year's survey also saw a continued rise in mobile as a major IT security challenge for organisations. We also questioned people about their approach to BYOD, another well-reported trend within business, and discovered that IT professionals are increasingly looking at BYOD as an IT security risk.

The conclusion is that IT security threats are now more 'silent', and at the same time more deadly. And, evidence shows that cyber-criminals are exploring low hanging fruit – targeting smaller and smaller businesses which lack the 'enterprise IT security' tools and skills to maintain a robust and real-time defence.

So while businesses across the world have made progress, Kaspersky Lab believes a major mindset change is needed.

IT security – are we worried about the right things?

1

The rise of mobile malware

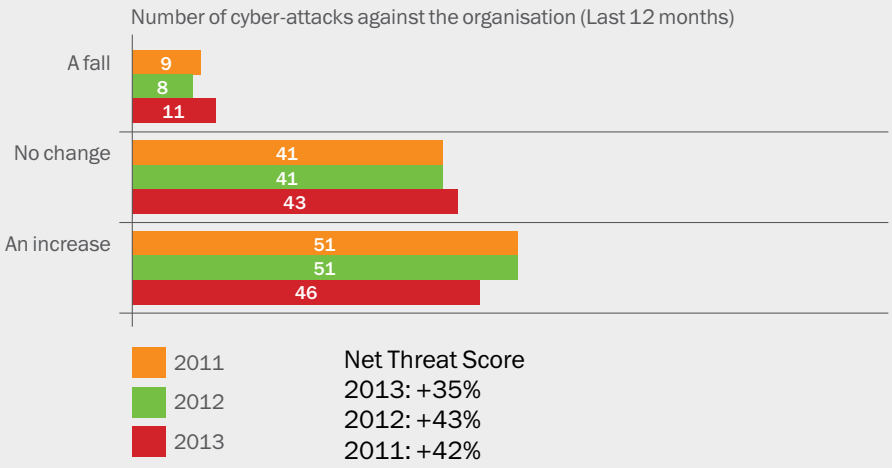
Number of samples in 2012 was 6x higher than in the previous year, which itself was equal to the previous six years.

This year's results were really a story of contradictions, which tells us that in a fast-changing IT security market with a complex threat environment, organisations are struggling to make sense of what to focus on, and where to prioritise their efforts and investments.

For example, the survey shows that there is a perception that the number of cyber-attacks is falling, but the reality is different. Only 46% of the surveyed IT decision-makers believe attacks are on the rise. Kaspersky Lab data shows that the volume of malware has continued to increase: currently tracking 200,000 unique malware samples every day. With mobile malware, this is also still growing, and at an exponential rate. The number of mobile threats tracked by Kaspersky Lab in 2011 was equal to the entire amount tracked in 2004-2010, and the amount in 2012 was six times higher than in 2011. In March 2013, over 9,000 new malware modifications were tracked.

Perceptions of number of cyber threats

The proportion perceiving an increase in attacks against their organisation has fallen in the last 12 months: set against the fact that security threats are actually increasing, this suggests a level of complacency may have set in.



Does this mean that the businesses are just that bit more prepared, so their perceptions are that the situation is improving (or at least not getting any worse)? Or that they just don't see IT security as a major concern? (Unlikely as the survey data suggests otherwise). Or, is it a more fundamental problem: that a concern over the volume of malware is not actually what organisations should be focusing on?

The vast majority of businesses (90%) drastically under-estimated the actual volume of malware. This problem is particularly severe in small businesses. Enterprises estimated the volume at 49,000 per day. Small businesses estimated even lower at 32,000 per day. So all businesses under estimate – to the tune of 60%+.

David Emm, Senior Researcher at Kaspersky Lab comments. **"Unfortunately this is not a simple issue. Volume of malware could be seen as a cause for concern but what should be of greater concern is the more sophisticated nature of the threats that businesses face today."**

As mentioned in the executive summary, this is one of the examples of where the difference in understanding and knowledge between SMBs and Enterprises is very noticeable.

SMBs rarely have IT security specialists on their payroll, and this reinforces the need for education and support in this sector, particularly as IT security and data protection once again took the top slots in the list of the most concerning issues for IT professionals. So they care about it, but haven't matched this with the right level of understanding and have fewer resources to deal with it.

"What was not understood was a realisation that malware has evolved. Criminal gangs use sophisticated malware to target organisations directly in order to steal valuable data. This connect is important, as stopping one prevents the other."

David Emm
Senior Researcher
Kaspersky Lab

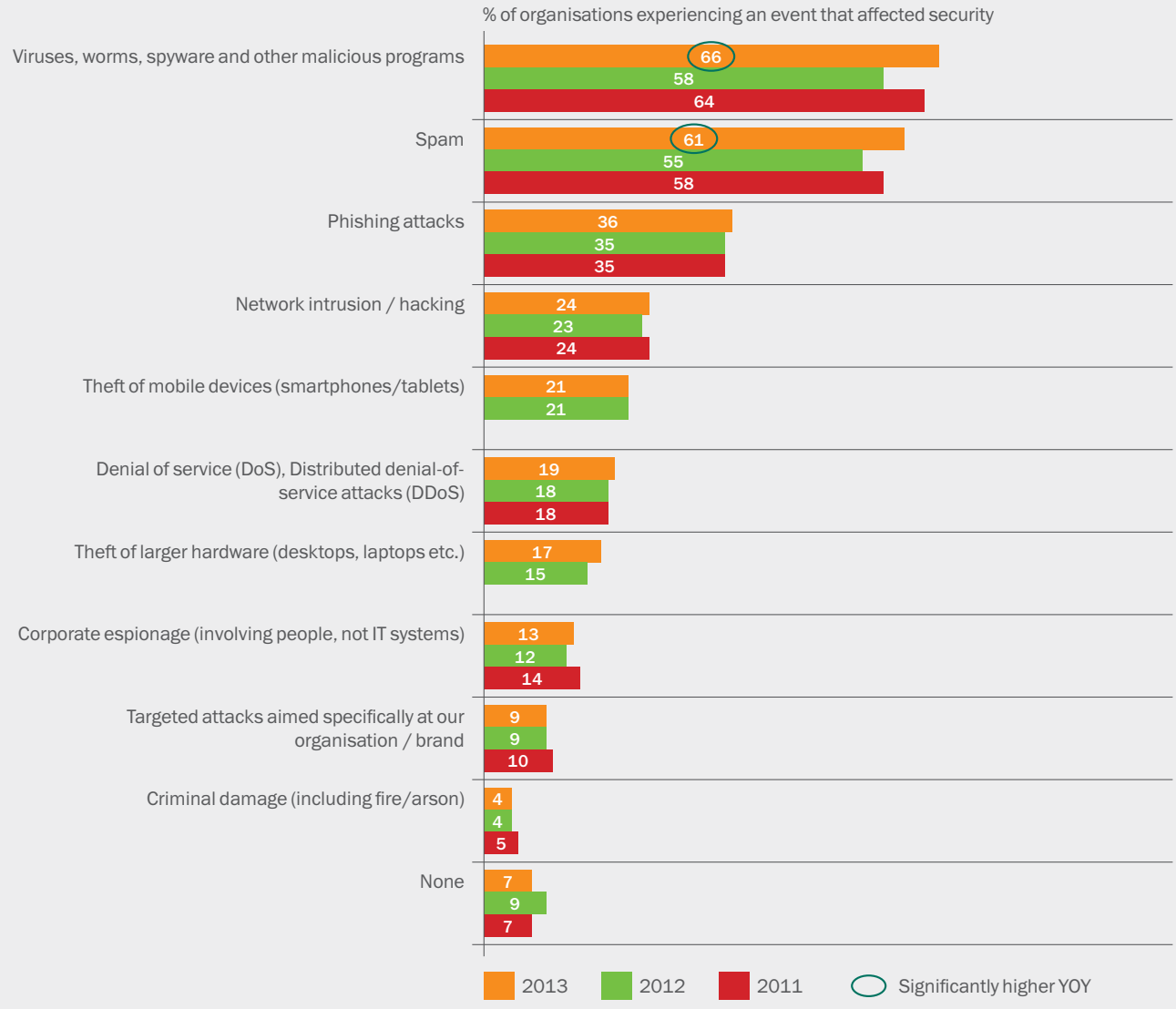
What is the real threat, really?

Every year, we ask IT decision-makers what threats they experience, and what they are concerned about from an IT security perspective.

Whilst 91% of businesses (unchanged from last year) have experienced at least one threat, and most (66% - up from 55% last year) have experienced viruses, spyware and other malicious programs; organisations are still not always making a connection between data loss and malware.

External threats experienced

91% of organisations have experienced at least one threat in the last 12 months. Malware is still the most common (and growing) threat. Theft of mobile devices continues to be a highly reported problem: 1 in 5 companies reported this as an issue they'd encountered within the last 12 months.



Business care most about customer information going awry, as this has a clear impact on reputation and therefore is a risk to the business. This was seen throughout all respondents regardless of company size and geography.

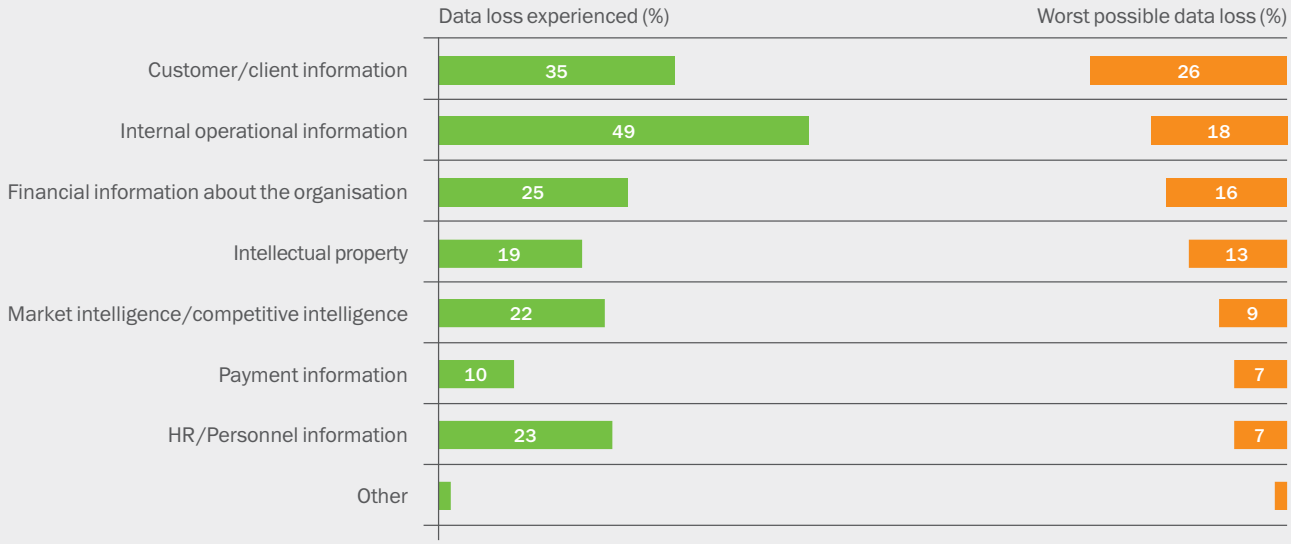
David Emm, Senior Researcher at Kaspersky Lab, comments: **"What has not been understood as clearly is just how far malware has evolved. Criminal gangs use sophisticated malware to target specific organisations in order to steal valuable data. This connection is important, as an effective strategy to stop one reduces the risk of the other."**

Understanding that malware is a major culprit of data loss would be a big step forward. It would make the fight against malware a higher priority within organisations.

Furthermore, when it comes to what IT professionals are worried about, incidents like 'network intrusion' featured highly in our survey. And what is causing network intrusion attacks? Malware – developed and deployed by criminals intent on stealing valuable data.

What is being lost and what businesses fear losing

Loss of client information is the leading concern for most businesses and is currently affecting 35% of those experiencing data loss in the last 12 months.



Managing the mobile madness

2

Only 1 in 10 say they have a fully implemented mobile policy across their organisation

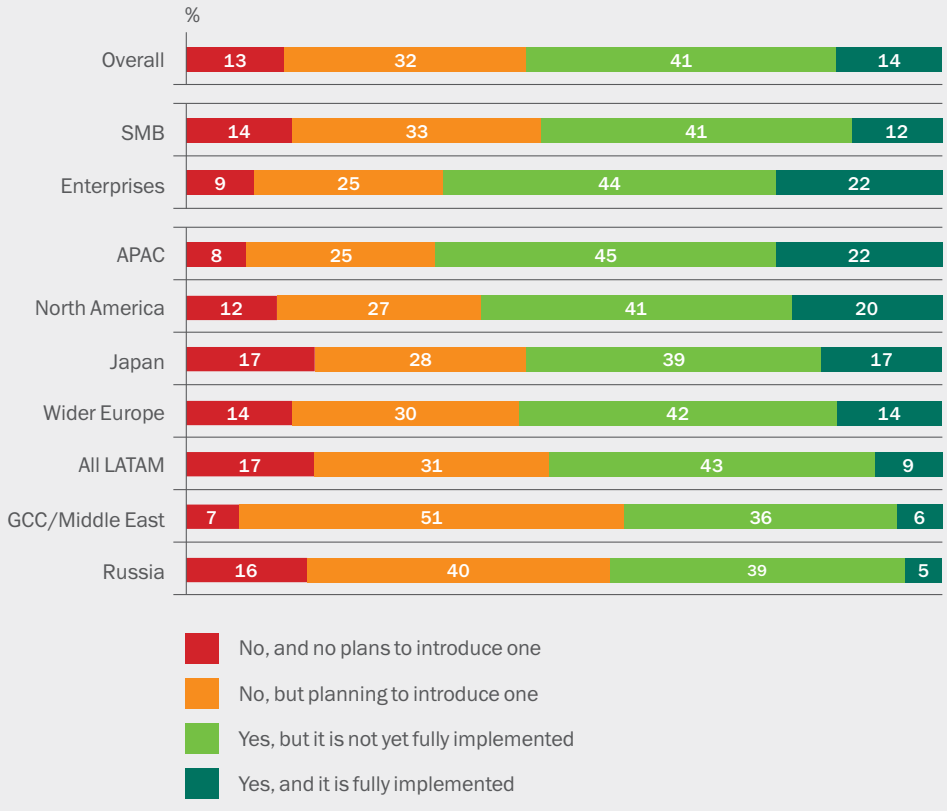
Following the statistical trend from last year's report, mobile continues to be an area of concern for organisations. Specifically looking at mobile, organisations' security concerns focus on the loss of sensitive business data (38%), overshadowing losing the device itself (33%).

However, what is remaining highly challenging for organisations is setting up and maintaining effective IT security policies for mobile devices and users. Only 1 in 10 say they have a fully implemented mobile policy across their organisation.

Clearly, IT decision-makers are finding mobile a difficult issue to address and 'bolt down'. Mobile, by its very nature, is harder to 'see' from an organisational perspective than a fleet of desktops or laptops. Added to that, how many of your employees have more than one phone? In today's increasingly consumerised world the blur between work and personal life means that company data of some description can all too easily end up on an employee's own device.

It security policy for mobile devices

Just over 1 in 10 companies have a fully implemented policy when it comes to mobile devices. Although there is a high level of willingness to adopt a policy, almost half have no policy at all.



Despite this, the proportion of organisations taking a proactive stance and deploying specific preventative measures is quite low. Only 24% of organisations are using Mobile Device Management software and only 40% use anti-malware for mobile devices.

Sergey Lozhkin comments, **"Mobile falls into the 'one more thing to manage' category. IT teams are rarely being given more funds or resources, despite their environment becoming more complex. Arguably, these teams are being forced into making uncomfortable compromises and not deploying the tools they'd like to because they require more resources to manage them."**

Another issue we saw was that for those 1 in 10 who had successfully implemented mobile security policies, very few of them received what they saw as the resources they needed to make this happen. We asked if they received an increase in budget to cover the extra task, and 16% said no, and another 48% said that the budget additions they received proved not to be sufficient.

However as mobile security matures, these barriers become more of a perception than reality. Today, mobile endpoint security platforms bring Mobile Device Management and mobile security into the same toolset, which therefore requires no extra IT skills and very little in the way of extra resources.

David Emm, Senior Researcher at Kaspersky Lab adds: **"In a way mobile is now a bit like email was when it first became widespread in organisations. Usage exploded and then IT teams had to retrofit the control tools and security policies. It feels to me as though we're at the same stage with mobile – and IT is only just starting on that retrofit operation."**

Bring your own device – is the tide turning?

3

This year we surveyed specific data points around own BYOD. We have seen this phenomenon grow rapidly in the last few years, largely fuelled by the rise in tablet ownership.

Most organisations globally have a relatively liberal 'own-device' usage policy. 32% allow unfettered usage (which means allowing use of company networks and resources) via smartphones, 29% via tablets and 37% via laptops. This last figure has dropped by over 10% from last year.

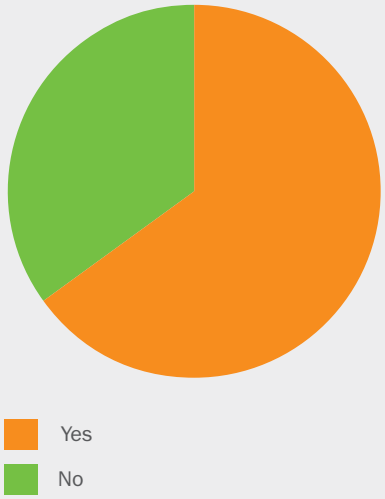
Unsurprisingly, we found that the larger the company, the stricter the restrictions. What was more interesting were the responses to a future-looking state. We found an overall hardening of sentiment among IT decision-makers when it comes to BYOD.

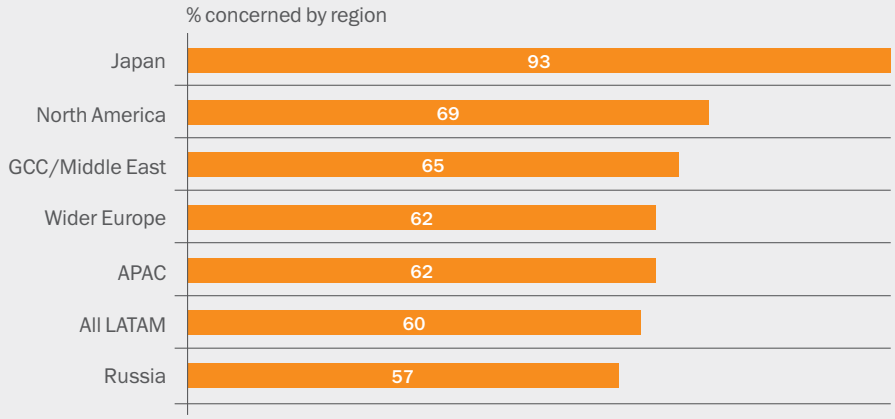
The survey clearly points to one major reason – IT security concerns. 65% of IT decision-makers felt that BYOD was a threat to the business. This was a fairly consistent phenomenon across the regions surveyed, with the one exception being Japan – where a stunning 93% expressed IT security concerns around BYOD. In addition, when we asked people to think ahead, 48% expressed a concern about how BYOD would cause risk in the future.

The perceived threat represented by BYOD

65% believe BYOD represents a threat to the security of their business; level of concern particularly high in Europe.

Is BYOD a threat to the security of your business?

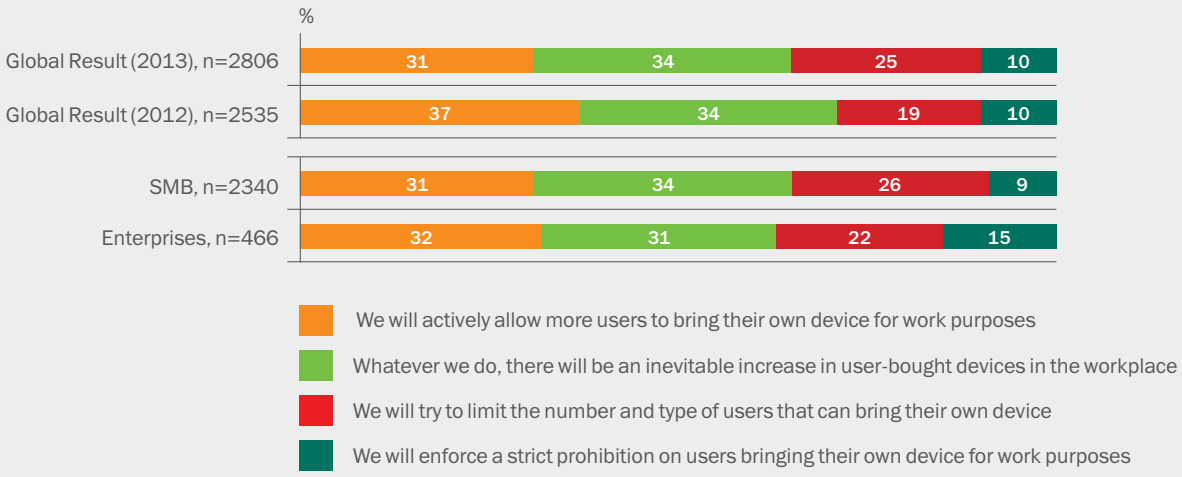




Costin Raiu, Director Global Research & Analysis at Kaspersky Lab comments. **"I think the tide could well be turning on BYOD. IT departments have been on the back foot. Tablet usage has exploded, especially at Exec level. So they had little choice but to let it happen. However, they're now witnessing the most sensitive of company data being held on own devices, and rightly see an IT security timebomb just waiting to go off."**

BYOD policy into the future

Only a small minority will restrict own device usage to any extent. However, the 2013 results that there is an overall hardening of sentiment among ITDMs when it comes to BYOD.



Looking broader – the management challenge

4

In the previous chapter, we looked at a changing attitude to BYOD. Looking at the survey data, it is clear that this is actually an indicator of a wider shift, and also a wider 'control' problem.

For example, just over half (54%) use patch management and systems management, despite them being among the most cited areas of technology challenges. In fact, the number using these fundamental management tools has dropped by 9% since last year's survey.

In addition, a worrying number of organisations' IT security 'strategy' was 'anti-malware only', and this approach was not restricted just to small businesses as you might expect.

Measures taken to avert security risks

Anti-malware protection is the most common, fully implemented security measure. Regular patch/software update management is still second, but implementation has fallen sharply since 2012 – this appears to be a big challenge faced by businesses across the world. Companies are adapting to dealing with security on the move for notebooks and remotely at other offices.

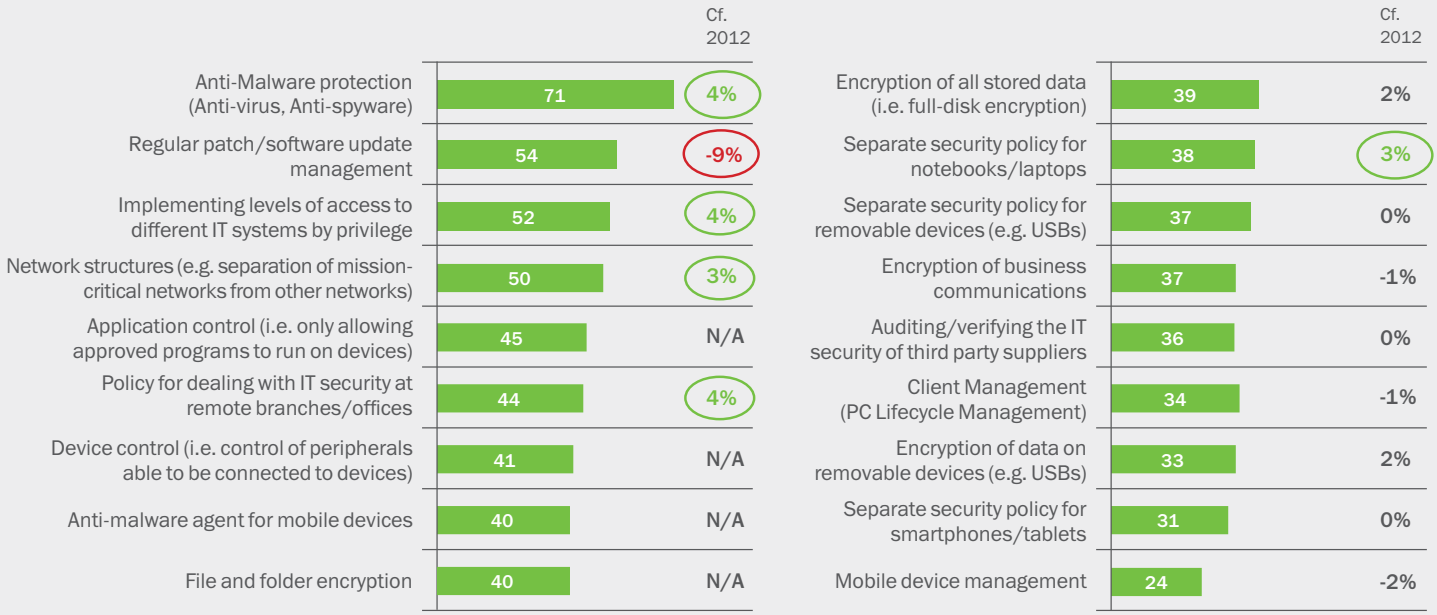


Chart shows % of organisations that have fully implemented different security measures

Significantly lower YOY

Significantly higher YOY

N/A – issues are new for 2013

Interestingly, we asked the respondents what technologies they felt they needed to understand more about, and 'understanding the range of management software currently available' was the second highest ranking at 51% (the highest being 'cloud' at only one per cent higher).

Sergey Lozhkin, comments. **"Systems management gives you visibility of what's going on in your network, what devices employees use and what programs are being installed. If you don't know what programs your employees download, install and use, you make yourself vulnerable to attacks and malware. It's a shocking fact that 80% of programs from file sharing sites such as Torrent are already infected with a virus!"**

David Emm continues: **"Systems management is perceived as difficult and/or expensive. This belief seems particularly strong in smaller organisations, who feel that it is an 'enterprise' technology. However, it needn't be. Today's unified security platforms deliver all the systems management functionality needed by SMBs, but without the cost or complexity typically associated with enterprise toolsets."**

Counting the cost of IT security breaches

5

- **60% of breaches resulted in some impairment of the business' ability to function**
- **53% experienced a negative impact on their reputation**
- **Financial damage is biggest in case of a temporary loss of ability to trade:**
  - **$1.7m for enterprises**
  - **$63,000 for SMBs**

For the first time in the survey's history we looked at quantifying the financial impact of IT security breaches.

This was no easy task, as in the past companies have been criticised for scare-mongering – using blunt calculations around the probability of a threat multiplied by an 'hourly downtime' figure. This approach lacks validity as there's no meaningful 'average' and IT downtime means different things depending on the type of business. An online retailer can go out of business very quickly in the event of a Denial of Service attack, for example. Whereas a professional services consultancy can still function as much of its 'trading' is conducted face to face and over a longer cycle time.

With that in mind, it's important to explain the methodology used in calculating the cost of IT security breaches.

- We asked all companies that reported a loss of data (whether sensitive orotherwise) about the impact of that event.
- We focussed our attention only on the company's most serious data breach within the last 12 months.
- Questions were asked about the various additional expenses and remedial and preventative actions that were taken as a result of the breach.
- Those that were able to comment upon the extent of the costs were asked about the estimated expense.

Using this data, coupled with some closer analysis of the reported business impact of data breaches, we make some estimates of the total costs of these events, across different sizes of companies and types of event.

The results are interesting, largely in part because they were based on real experiences, not hypothetical situations. In nearly all cases (88%) some form of paid professional services was required to fix the problem – usually IT security consultants, but lawyers also figured highly on the list. For enterprises the average cost of this was $103,000. SMBs paid out on average $13,000, which for a small business is a significant unplanned cost item.

A high proportion (60%) of breaches resulted in some impairment of the business' ability to function, and 53% reported a negative impact on their reputation. This cost (which is less precise as it involves more 'intangible' factors in some instances) was higher; $150,000 for enterprises and $22,000 for SMBs.

The biggest financial loss factor, however, is when an IT security breach causes a temporary loss of ability to trade. This was a rarer occurrence in the businesses we surveyed, but the costs the incurred were significant; $1.7m for enterprises and $63,000 for SMBs.

We then explored what preventative measures would then cost – bearing in mind this is for organisations that have had a data loss event and need to increase their IT security by some significant degree. 59% invested in extra software or hardware infrastructure, 49% invested in staff training and 38% actually hired extra staff (this was more common in enterprises, less so in SMBs).

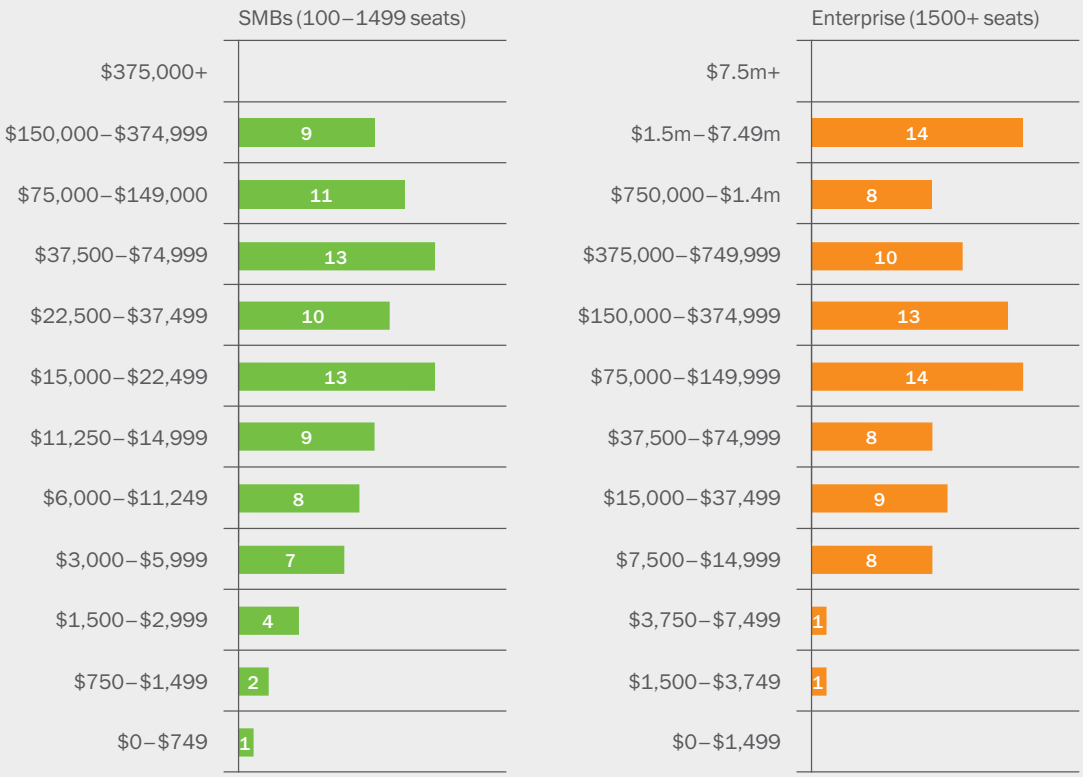
So where do we get to if we add all this up, taking into account the varying levels of probability of certain costs occurring (low probability for 'loss of ability to trade' for example)? Conservatively, and looking only at figures that our respondents could easily and quickly measure, the cost impact of a data security breach is around $649,000 for enterprises and $50,000 for SMBs.

David Emm, Senior Researcher at Kaspersky Lab comments. **"These figures really show the cost of IT security breaches in a new light. If organisations were aware of this real cost, then I think businesses would behave very differently. For me, this highlights the need for better education and awareness of the potential risk, as well as the need for effective technology."**

Additionally, elsewhere in the survey, it was clear that organisations were not as focused on end-user education as they should be. Many targeted attacks arise due to employees not understanding the threat, not knowing what to look out for, what might be suspicious, and how their actions might compromise the security of the company they work for.

Total cost of lost business opportunities

The median cost of lost business opportunities due to a serious data loss event is $22k for SMBs and $150k for enterprises.



Recommendations – time to step up a gear

6

Don't mistake lack of noise for lack of threat

A virus is no longer something that just 'slows up your machine'. Today's threats are sophisticated and designed not to be noticed. This isn't really about complacency, it's about recognising that IT security has fundamentally changed in nature.

Bring mobile and BYOD under your control

The rush to buy tablets isn't going to end soon, and organisations should make it a priority to get this under control from a data security perspective. This is partly about setting strict policies on BYOD, partly about staff education and partly about implementing a plan to secure mobile working. When data's on the move, it is at risk.

Anti-malware is no longer enough – move to a deeper level of control

This year's survey showed that uptake of patch management and systems management have actually dropped. Other areas such as data encryption and mobile device management are still relatively low in usage. Given that criminals are increasingly using sophisticated tools to harvest valuable data – a deeper level of control and protection is needed. The tools exist, and can be just a natural extension of existing anti-malware, so businesses really need to step up.

Focus on improving IT security management – through a single console

Following logically on from the previous point, there are more issues and more technologies to consider, so management needs to be consolidated through a single console. Only by doing this can organisations with finite resources hope to improve their overall security posture.

Education, education, education.

One constant in this year's survey has been the lack of staff awareness or concern about IT security. Around 40% of companies said that their employees tend not comply with IT security policies or even understand why they are in place.

This has to change and as a global community of IT security professionals we all must take responsibility for making this happen, fast.

We must educate employees and show them how their activity and behaviour could impact the organisation they work for, and also their own personal information. Give them the key things to remember and they will have a lasting positive effect on an organisation's IT security posture.

With Kaspersky, now you can.

Kaspersky Lab is one of the fastest growing IT security vendors worldwide, and is firmly positioned as one of the world's top four leading security companies. An international group operating in almost 200 countries and territories worldwide, we provide protection for over 300 million users and over 200,000 corporate clients, ranging from small and medium-sized businesses all the way up to large governmental and commercial organisations.

We provide advanced, integrated security solutions that give businesses an unparalleled ability to control application, web and device usage: you set the rules and our solutions help manage them.

Kaspersky Endpoint Security for Business is specifically designed to combat and block today's advanced persistent threats at every turn and, deployed in conjunction with Kaspersky Security Center, gives security teams, the administrative visibility and control they need – whatever threats emerge.

Find out at more at kaspersky.com/business

Meet our experts

The expert insight in this report is provided by Kaspersky Lab's Global Research and Analysis Team.

David Emm
David first joined the anti-virus industry in 1990 and moved to Kaspersky Lab in 2004, where he conceived and developed our Malware Defence Workshop. He is currently Senior Regional Researcher, UK and is a regular media commentator. His key research interests include the malware ecosystem, ID theft, and Kaspersky Lab technologies. David's blog can be found at www.securelist.com/en/blog?author=55

Costin Raiu
Costin is the Director of the Global Research and Analysis Team. Formerly Chief Security Expert, Costin has been with Kaspersky since 2000 and specialises in malicious websites, browser security and exploits, e-banking malware, enterprise-level security and Web 2.0 threats. Read his blog at www.securelist.com/en/userinfo/62 or follow @craiu on Twitter.

Sergey Lozhkin
Sergey is a technology expert for Kaspersky Lab. Graduated in 2002 from Omsk Law Enforcement Academy and worked as a Detective within the Cybercrimes investigation Unit in Omsk city police department. After leaving government service in 2004, Sergey worked in IT security for several different companies as an IT security specialist, and engineer. Also working as a penetration tester, he performed penetration research for various government and private company networks.

With Kaspersky, now you can.
kaspersky.com/business

Be Ready for What's Next

KASPERSKY lab