Exclusive 2014
Survey Results

IT Security Threats and Data Breaches

Perception versus Reality: Time to Recalibrate

Empower business through security.
kaspersky.com/business

#securebiz

KASPERSKY lab

Contents

About the Global IT Risks Report

Now in its 4th year, **Kaspersky Lab's Global IT Risks Report** collects insights from IT professionals around the world. Conducted by research specialists B2B International and analysed by Kaspersky's expert threat intelligence and research teams, the report is an essential look at the industry's prevailing attitudes and strategies towards IT security. It also serves as an industry benchmark to help businesses understand the type and level of IT security threats they face.

Why read this report?

- **It spans global and cross-sector findings**
- **It gives you exclusive insight into the views, opinions and strategies of IT professionals from around the world**
- **It helps you benchmark your IT security against industry peers**

Global IT Risks Report 2014:

Executive Summary

The survey in summary:

- **3,900 respondents**
- **27 countries**
- **Concerning April 2013 to May 2014**
- **Surveyed IT professionals with a 'good working knowledge' of IT issues**

During 2013 and 2014, IT security has intensified from a 'concern' to a 'global news story', where data leaks, corporate espionage and cybercrime have frequently hit the headlines. But what's really going on behind all the hype and how does it affect you?

With global markets beginning to return to better economic health, longer-term strategic considerations are again high on the boardroom agenda. A renewed focus on growth and not simply surviving the next financial year has caused a shift in priorities – and increased attention is now being paid to risk management strategies. But these strategies are only effective when they're built on an accurate understanding of the current threat landscape.

One of the most interesting things this year's survey highlighted is what we're calling **'the perception gap'**. That is, the difference between our perception of what's happening and the reality on the ground.

During 2013 and 2014, Kaspersky Lab detected around 315,000 daily malicious samples. Of those businesses surveyed, only **4%** were able to accurately state this figure. In fact, **91%** of respondents underestimated it and **70%** guessed that there were less than 10,000 daily threats. A serious miscalculation.

But this is only part of the story. **94%** of companies have experienced some form of external security threat, and yet only **68%** have fully implemented anti-malware on their workstations and only **44%** employ security solutions for their mobile devices.

94% of companies have experienced some form of external security threat

So, how do we fix this? We need to recalibrate our perceptions of the industry to better understand the threats. And not just the visible security breaches, but the daily and ongoing security risks too.

A big concern is the control and integration of mobile devices into normal working practices, and security relating to virtualization. However, only **34%** of IT decision makers have a clear understanding of the virtual security solutions available, and **46%** of businesses think that their conventional security solutions provide adequate protection.

The **estimated** impact of data breaches for small and medium-sized businesses (SMBs) dropped by **12%**, from **$54,000** to **$48,000**, but the estimated impact on enterprise-sized businesses rose by **14%** from **$700,000** to **$798,000** but this could well be a perception issue. Enterprises are larger and better equipped to detect breaches, whereas small and medium-sized businesses (SMBs) may not know when they've been under attack.

But this impact isn't as simple and straightforward as we might think. **87%** of businesses that suffered data loss required additional professional services of some kind and nearly half **(47%)** incurred significant additional costs. Last year, the average 'typical damage' (hiring professional services, increased downtime and lost business opportunities) to SMBs from a serious event was $35,000. For enterprises, this figure was $690,000.

The impact that data breaches can have on trust and reputation was also very apparent. **82%** of businesses would consider leaving a financial institution if it suffered a breach, while **27%** don't think that banks are doing enough to secure their financial information.

82% of businesses would consider leaving a financial institution if it suffered a breach

There is a split though, in the perception of who is ultimately responsible for securing financial transactions. Only **35%** of customers think that financial institutions are primarily responsible, whereas **85%** of financial institutions felt that they themselves were responsible.

So what's the story? Well, businesses are making progress, but so is the cybercrime industry. Though the tools exist for organisations to protect themselves, most businesses are still taking a reactive approach to IT security. They need to be more proactive and stop underestimating the diversity, number and sophistication of today's threats. To put it simply, traditional anti-virus solutions aren't enough anymore.

Businesses need to recognise the complexity of the challenge ahead. Building a multi-layered defence against the threats posed by 'human' factors, the sprawl of multiple devices and the emergence of new technologies is now essential as no business has sufficient human resources to handle it all.

It's time to undertake a serious recalibration of how security issues are perceived and tackled. Businesses need to be more proactive and vigilant, and they need to educate themselves – or risk becoming the next big IT security news story.

To put it simply, traditional anti-virus solutions aren't enough anymore

Global IT Risks Report 2014:

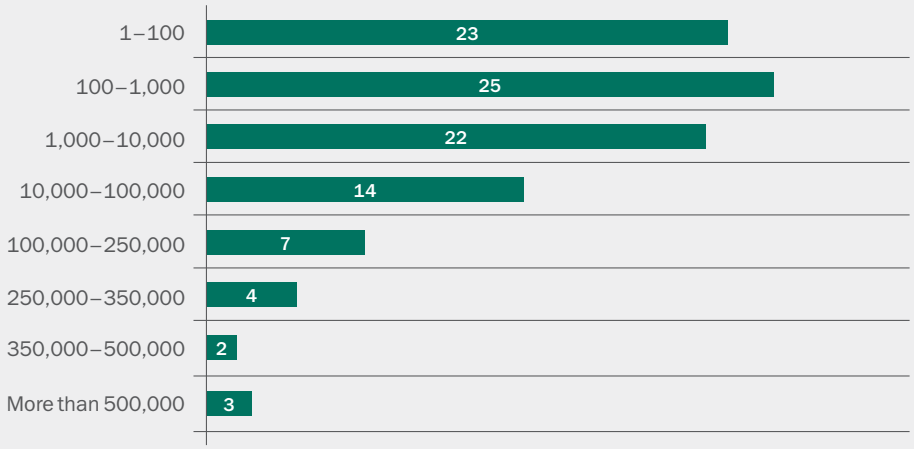
1 Perception vs reality – how do we close the gap?

> **There's an increasing gulf between what businesses believe the threat landscape to be and what it actually is. We've called this the 'perception gap'. It shows that organisations, no matter what their size, wildly underestimate both the amount and severity of the threats they face.**
>
> Costin Raiu, Global Research & Analysis Team, Kaspersky Lab

As an IT decision maker, you're responsible for your business-critical systems and infrastructure. You protect your business against threats, prevent data loss, and ensure everything performs optimally. And most of the time, you get it right. But what about the occasions when you don't? What about the things you miss?

Sometimes you need a reality check to help, and you need to adjust your views to reflect the ever-changing and evolving nature of the threats you face. **91%** of business decision makers underestimate the number of threat samples discovered daily, and only **4%** have an accurate idea of the actual number that exist. More to the point, most of us dramatically underestimate this figure, with **70%** believing there are less than 10,000 new samples discovered daily. The actual figure, as detected by Kaspersky Lab, is 315,000 new samples.

Perceived Number Of New Malware Samples Discovered Daily (%)



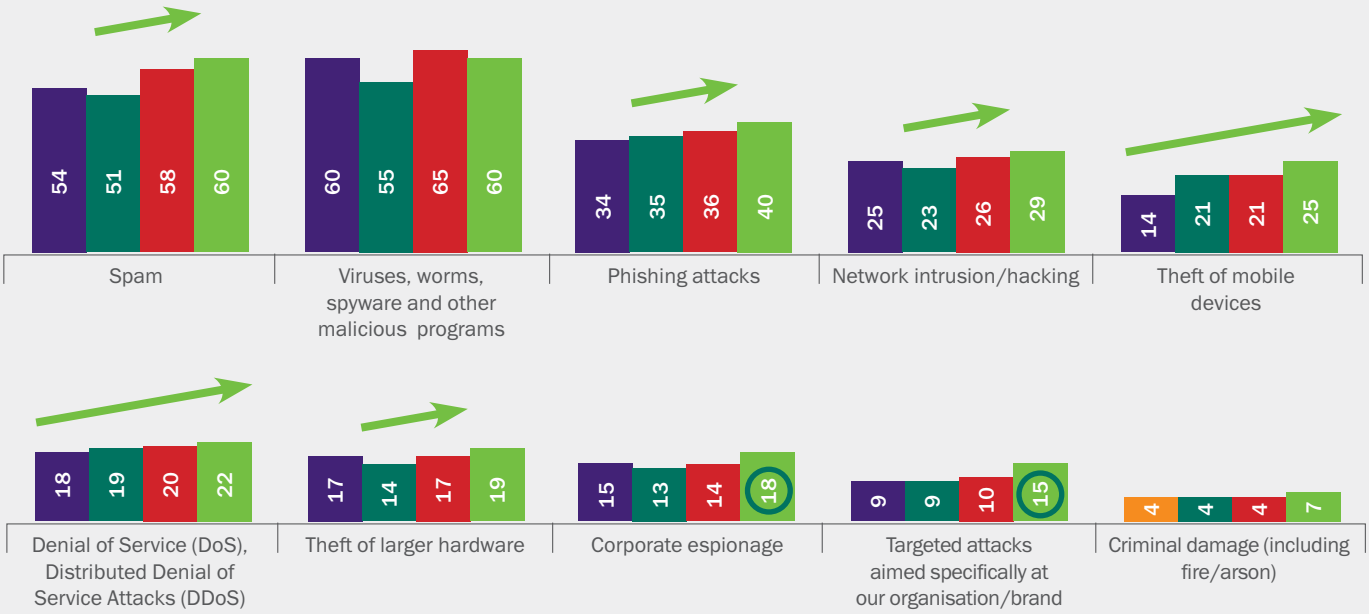
Surprisingly, despite underestimating the number of threats, participants in the survey reported a perceived increase in the number of cyber-attacks every year for the last 4 years. This could be down to many organisations thinking there's been an increase in threats relating to them, but not having a clear idea of the overall picture.

Businesses of all sizes have reported rising levels of spam, phishing and DDoS attacks as areas of concern. Corporate espionage and targeted attacks are also on the increase. The number of organisations reporting specific attacks targeting them directly has increased by **5%** from 2013, and now stands at **15%**.

So what sits behind all of these threats?

External Threats Experienced

94% of companies had experienced some form of external threat. There are also some clear trends emerging, such as the steady increase in Denial Of Service Attacks over the last four years.



A big misconception is that malware is something specific and discreet, rather than something that's actually integrated into cyber-attacks. Though reported malware attacks actually decreased between 2013 and 2014, they remain the most numerous and dangerous threats to IT security. Phishing, DDoS and targeted attacks are all connected by their use of increasingly sophisticated malware.

And while there are a number of security measures already being taken, there are still large gaps in IT security systems, regardless of business size.

Despite the nature of the threat posed by malware, only **68%** of businesses deploy anti-malware software on their workstations, only **42%** use mobile security solutions, and only **52%** of all businesses surveyed regularly patch or update software – an important task in preventing malware attacks or data breaches.

At best, this suggests that businesses are only partially protected; a more critical reading suggests that they're woefully underprepared for the threats they face.

So how do businesses close the gap? Through a better understanding of the true nature of these threats and by effectively deploying and maintaining targeted security solutions.

Global IT Risks Report 2014:

2 More sophisticated threats require multi-layered protection

Right now, organisations around the world are facing increasingly complex security threats. And sadly, it's no longer the case that one product or approach can protect them from all types of malware, virus or malicious program. A 'one size fits all' policy lacks the scope and ability to safeguard businesses from multiple attacks on their IT infrastructure.

Making matters worse, malware is quick to evolve and changes on a daily basis. It's like fighting a hidden enemy that's constantly moving. At the end of 2013, there were 200,000 unique mobile malware code samples. In the first half of 2014 alone, a further 175,000 new samples were created. Quite alarming growth rates, and something to consider when it comes to defining your security strategies for data protection, financial transaction security, and maintaining service continuity against DDoS attacks.

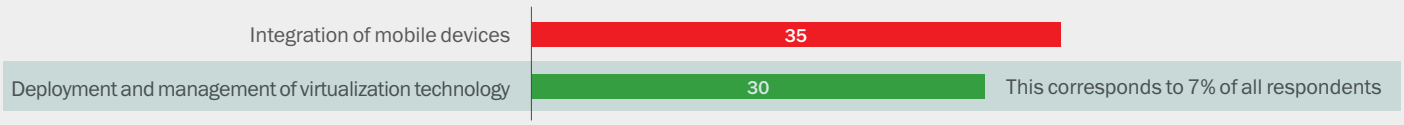
> **One of the most concerning survey stats is the very low usage of application and patch management. Given that the majority of all security breaches stem from an unpatched application vulnerability – this has to be a key focus area for any IT professional.**
>
> Sergey Lozhkin, Global Research & Analysis Team, Kaspersky Lab

It's worth noting that what's best for one business isn't necessarily best for another. It's essential to get the right solution for your business's network, whether you run LAN, wireless and cellular networks, wide area networks or IP-based communications, or a combination of these. Security solutions need to operate effectively across these platforms without compromising on security or performance. And with virtualization high on the agenda for many companies, and the increasing role of mobile devices in business, it's now more important than ever that organisations understand the need for multi-layered, integrated threat protection that works across physical, mobile and virtual devices.

From the chart below, we can see that of those respondents who felt 'managing change' was a top concern, **30%** said that the deployment and management of virtualization technology was their biggest challenge, while **35%** said that for them it was the integration of mobile devices.

MANAGING CHANGE IN IT SYSTEMS

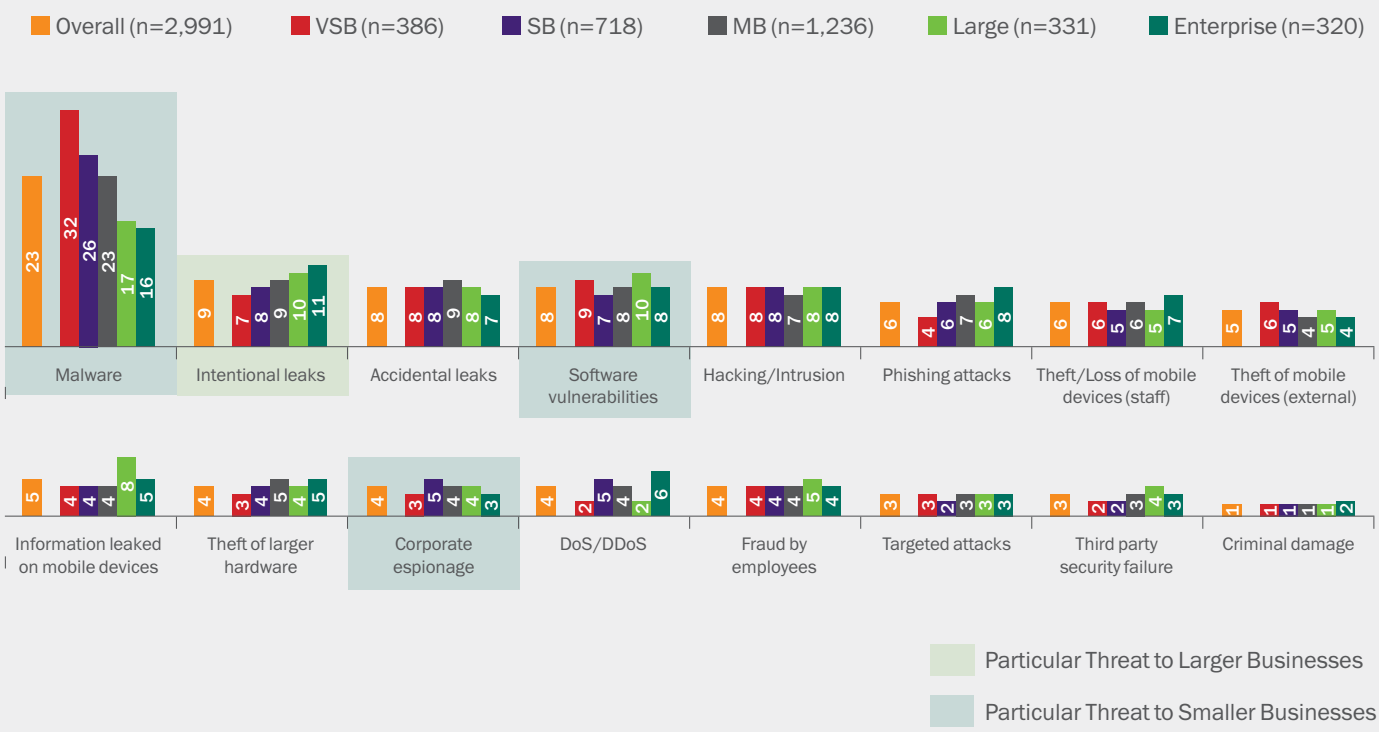
Looking at the 22% of respondents who felt managing change was a top concern in more detail, mobile and virtualisation are key challenges



The next chart highlights the threats to both large and smaller businesses – from malware and data leakage through to corporate espionage and mobile device theft.

MOST SERIOUS DATA LOSS EVENT

Malware is currently the leading cause of serious data loss events. It's less of a problem for larger businesses, where the intentional leaking of information is much more of a concern.



Base: Varies All Respondents Of Each Size Who Lost Data

From the chart above, it's evident that malware is the biggest cause of data loss. So why is it that, from 2013 to 2014, businesses perceived a **5%** drop in malware attacks? Well, to put it simply, **91%** of businesses underestimate the number of new samples discovered on a daily basis, and it's not widely understood that lots of targeted attacks, like phishing and DDoS, actually have malware at their core. So it's not that malware infiltrations have decreased, it's that attacks may not be perceived as malware attacks.

So what can we take from these findings?

1. Traditional anti-virus solutions are no longer effective and don't provide the depth and scale of protection that businesses require.
2. The growing complexity of IT infrastructure provides more opportunities for malicious attacks.
3. Human error and misjudgement can't be ignored, and the increase of Bring Your Own Device (BYOD) has made it easier to exploit working practices.

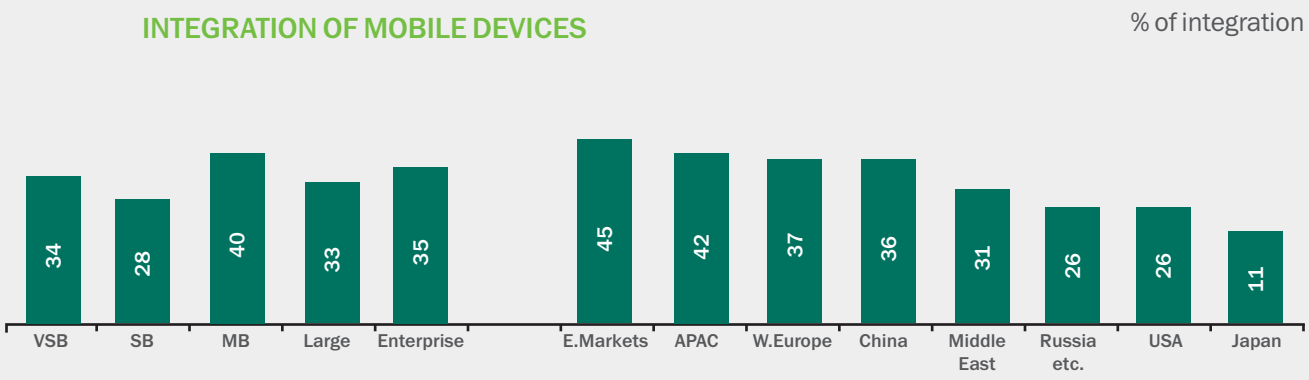
3 Global IT Risks Report 2014: Mobile threats now being realised

Mobile working is being rapidly adopted by businesses across the world. But its strength – namely helping the workforce to be more flexible – is worth nothing if the right security measures aren't put in place. An unprotected mobile device provides access to sensitive data and gives cybercriminals an easy point of entry to an otherwise secure system.

That's why **35%** of businesses recognised that the integration of mobile devices was one of their biggest challenges for the year ahead. And it's not just a hot topic for larger businesses. The integration of mobile devices is essential for businesses of all sizes, as the chart below shows us. It's only small businesses, at **28%**, that have less than a third of respondents listing mobile integration as a top concern. However, this could be due to small businesses underestimating the potential threats to and from mobile devices.

24% of businesses listed BYOD as one of their biggest IT security priorities over the next 12 months, and this figure rose to 32% among very small businesses. This shouldn't really come as a surprise, given that **42%** of businesses currently conduct sensitive transactions on their mobile devices.

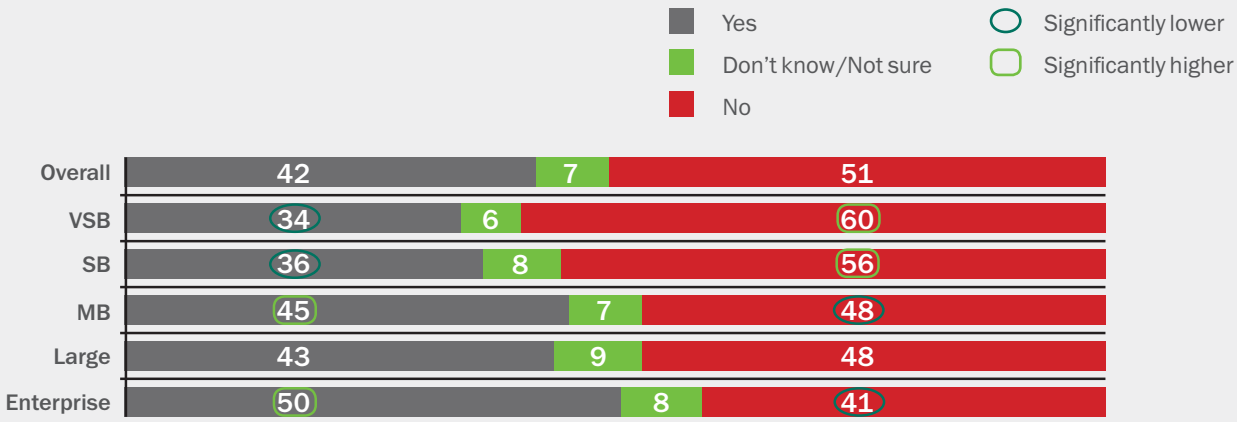
INTEGRATION OF MOBILE DEVICES



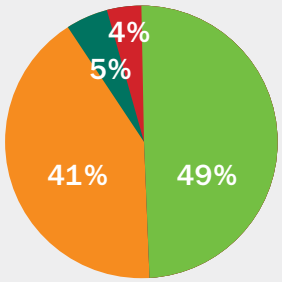
> **We all know that businesses are more mobile, but the usage profile is changing – you now see most businesses using mobile devices to share sensitive information and even conduct financial transactions.**
>
> David Emm, Kaspersky Lab, Global Research & Analysis Team

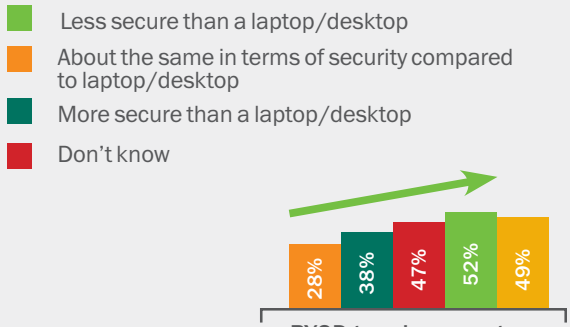
USAGE AND ATTITUDES TOWARDS MOBILE TRANSACTIONS

Does your business conduct sensitive transactions on mobile devices?



How secure are transactions on mobile devices?





BYOD trends present an increased IT security risk to our business.

What could come as a surprise, however, is that just under half **(49%)** think mobile devices are less secure than a laptop or desktop computer. **41%** think their mobile device was just as secure as their laptop or desktop, **5%** said their mobile device was more secure, and **4%** didn't know.

It's interesting to see that all businesses view BYOD as a threat to their security. But this perceived threat changes with the size of the business. Basically, as the company size increases, so does its concern over BYOD security risks. **28%** of very small businesses believe it presents an increased threat, rising to **47%** and **49%** for medium-sized businesses and large enterprises respectively.

And they'd be right in thinking this, too. Over the last four years, **30%** of companies have experienced the theft or loss of a mobile device. And although data loss resulting from this has fallen in the last two years, from **26%** in 2012 to **21%** in 2014, it's still the second-highest way for a company to lose its data, beaten only by its staff accidentally sharing data.

Over the last four years, 30% of companies have experienced the theft or loss of a mobile device.

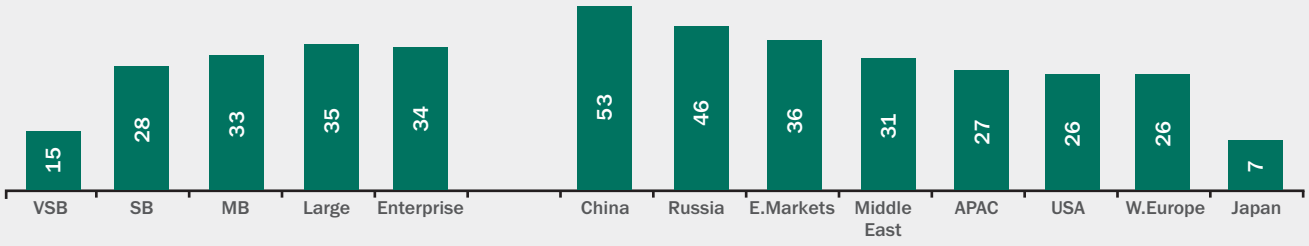
Global IT Risks Report 2014:

4 Virtualization – Protecting new working environments

For many companies, virtualization has been a part of their IT strategy for some time, but the actual implementation of specific virtualization security measures is low. It's an issue on a lot of people's minds – and was mentioned as a key IT security priority for the next 12 months by **14%** of companies surveyed (a figure rising to **21%** of enterprise-sized companies).

DEPLOYMENT AND MANAGEMENT OF VIRTUALIZATION TECHNOLOGY

% stating each as a change managemnet challenge they are currently dealing with.



> **Virtualization is an increasingly important part of most businesses' IT strategy. But when it comes to adopting specialised security solutions, too few have a clear understanding of the solutions available or the security requirements that a virtualized environment creates.**
>
> Sergey Lozhkin, Global Research & Analysis Team, Kaspersky Lab

Virtualization is more of a concern for large businesses and enterprises than smaller companies. Over a third of medium, large and enterprise-sized businesses listed it as a key challenge, compared to **28%** of small businesses and **15%** of very small businesses.

The understanding of virtualization security options is mixed, even among IT professionals. Only around a third of organisations surveyed possess a clear understanding of the solutions available and approximately a quarter have either a weak understanding or none at all.

GLOSSARY:

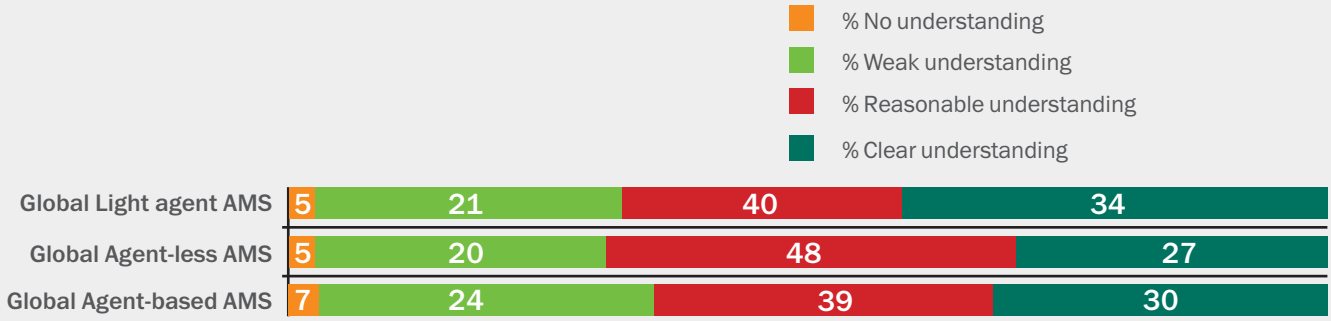
The three types of anti-malware software available for virtual networks offer different security options and are best deployed in different ways.

Agent-less: Based on push technology and centralised design. Controlled by a central console and doesn't require agents to be installed on individual or virtual machines. It can lower costs, reduce management and is easily deployed across large enterprises.

Agent-based: Based on pull technology and requires client side software before providing a server with updates. Agent-based solutions are good for roaming users or disconnected machines, and can be a useful complement to agent-less solutions.

Light agent: Operates by rerouting heavy workloads to a virtual appliance while securing endpoints against threats. Light agent is a mix of agent-less and agent-based.

UNDERSTANDING OF VIRTUAL ENVIRONMENT SECURITY SOLUTION AMONG SECURITY EXPERTS



24% of companies think that their existing anti-malware software provides better protection and, importantly, better performance than specialised solutions. **20%** stated that they didn't have any problems with their traditional solutions and **13%** felt that the threat to their virtualized environments was not sufficient to justify the additional cost of implementing a specialist solution.

Despite a very mixed understanding of the security options available to them, **52%** of businesses surveyed agreed with the statement that **"Virtualized environments increasingly form a core part of our critical IT infrastructure."** So, as they become a core part of a business's working practices, they have to be efficient and secure, but it's clear that a process of education is needed if they are to be secured effectively.

The overall picture is that companies seem unprepared to change their security requirements when they're implementing virtual environments. These include increasing their understanding of virtualization security and the adoption of specialised security platforms. Both of which are crucial to security in this area.

5 Global IT Risks Report 2014: Anti-fraud – counting the cost

Fraud prevention is near the top of many companies' agendas. **63%** of respondents agreed with the statement, **"We make every effort to ensure our anti-fraud measures are up-to-date"**. This figure was at least **10%** higher than those concerned with mobile integration, virtualization, DDoS attacks and other key IT strategy issues.

However, **43%** of organisations still feel that they need to improve how they secure their financial transactions with their bank.

And these fears are well founded. In 2013, the number of cyber-attacks involving financial malware increased to 28.4 million – 27.6% more than 2012.[1] In the same period, Kaspersky Lab protected 3.8 million users from financial attacks, and blocked more than 330 million phishing attacks.[2]

In 2013, the number of cyber-attacks involving financial malware increased to 28.4 million – 27.6% more than 2012.[1]

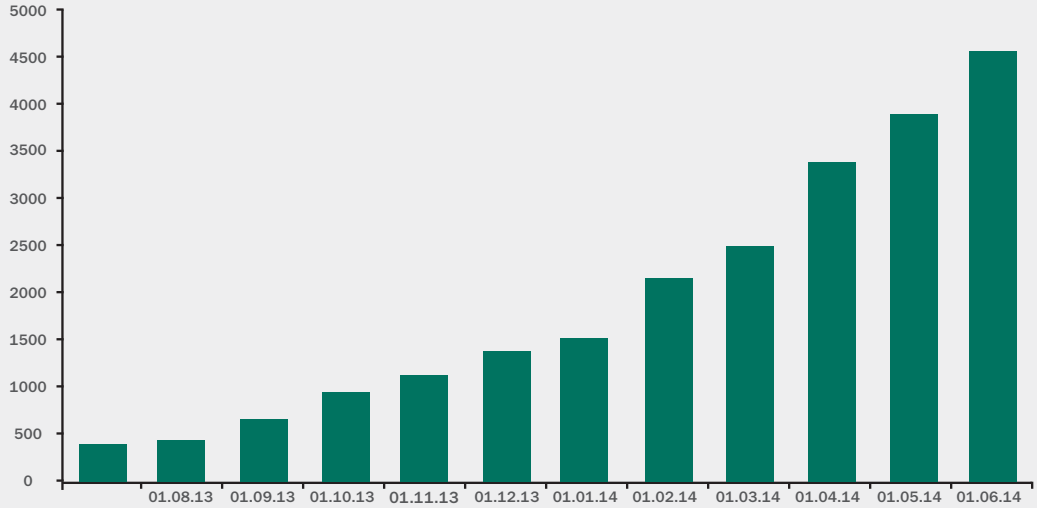
MOBILE BANKING TROJANS

Mobile malware is designed to make cybercriminals money. They operate alongside Windows-based Trojans and bypass traditional authentication techniques, attacking and stealing mobile transaction numbers (mTANs) issued by banks – allowing illegal transfers of funds.

There has been a sudden and sizable growth in autonomous Android banking Trojans in the past 18 months – from just 67 banking Trojans at the start of 2013 to 1,321 by year end, and an additional 3,215 recorded by the middle of 2014.[3] While these attacks have, so far, been mainly targeted at users in Russia and the Commonwealth of Independent States, it's likely that cybercriminals will continue to develop their techniques, expand their reach and move into new markets.

1. http://www.kaspersky.com/about/news/virus/2014/Kaspersky-Lab-statistics-attacks-involving-financial-malware-rise-to-28-million-in-2013
2. http://securelist.com/analysis/kaspersky-security-bulletin/59414/financial-cyber-threats-in-2013-part-2-malware/
3. http://securelist.com/analysis/quarterly-malware-reports/65340/it-threat-evolution-q2-2014/.

NUMBER OF BANKING TROJANS DETECTED, Q2 2014



Source: http://securelist.com/analysis/quarterly-malware-reports/65340/it-threat-evolution-q2-2014/

Well-known examples include ZeuS-in-the-Mobile (ZitMo), SpyEye-in-the-Mobile (SpitMo), Carberp-in-the-Mobile (CitMo) and Svpeng. Svpeng is an Android Trojan that steals the login and password details from a user's mobile banking app. It can also steal information about the user's bank card by prompting the user to enter their bank details when Google Play is opened. In the three months of the Trojan's existence, Kaspersky Lab discovered 50 of its modifications and blocked over 900 installations[4].

Financial markets are built on trust – trust that obligations will be fulfilled, payments made and data protected. So it's no surprise that protecting their reputation and track record are key concerns for businesses involved in financial data security.

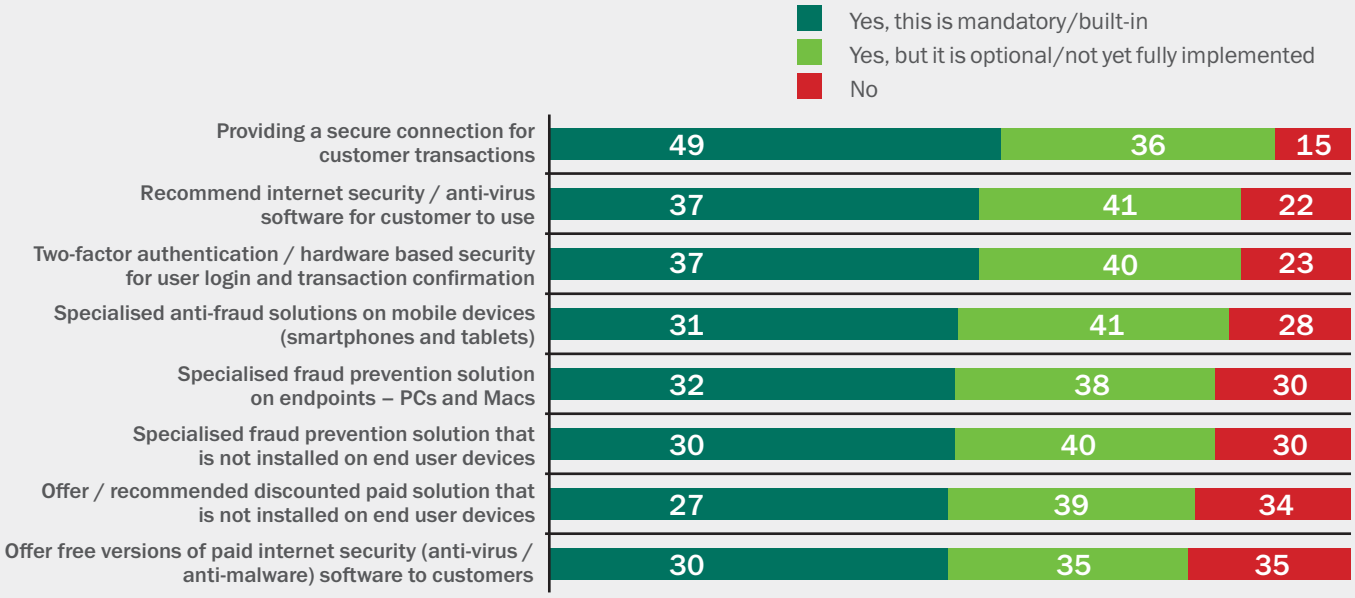
73% of businesses were influenced by a bank's security reputation when deciding who to work with, and **82%** said that they would consider leaving a bank if it suffered a data breach. This shouldn't be a surprise – taking an organisation's reputation into account is good risk management. Nor should it be a surprise that protecting customer data is high on the agenda for the companies surveyed. Perhaps more interesting, though, is that **18%** would tolerate a security breach relating to their financial security.

Rather alarmingly, just over half **(51%)** of all businesses surveyed felt that financial organisations were doing enough to protect their financial information. So just what are financial service providers and e-commerce operators doing to protect their customers and prevent fraud?

The survey spoke to over 2,500 companies working in this space and the results mostly show an industry in transition. While nearly half of respondents offered a secure connection, roughly a third were either still implementing a secure service or didn't enforce it, and a further **15%** offered no secure service at all. For the remaining ways of securing transactions, the majority of organisations were either in the process of delivering capabilities, offering optional anti-fraud measures, or hadn't implemented them at all.

4. http://securelist.com/blog/research/57301/the-android-trojan-svpeng-now-capable-of-mobile-phishing/

ANTI-FRAUD MEASURES EMPLOYED BY FINANCIAL SERVICES PROVIDERS & E-COMMERCE OPERATORS



BASE: 2,680. All respondents in financial services or operating online, public

Banks and customers have differing views on who is responsible for financial security. Only **35%** of customers thought that financial institutions carried the ultimate responsibility for financial security, compared to **85%** of institutions themselves. Very small and small businesses were the most inclined to believe that responsibility lay with the financial institution – **48%** and **41%** respectively – compared to only **27%** of enterprise-sized organisations.

Given the lack of dedicated security teams in small businesses, IT personnel have to take full ownership for securing the process and the responsibility for its failures. **28%** of customers thought that their IT department carried the ultimate responsibility. This further highlights the need for multi-layered, fully integrated protection that's capable of covering the full range of SMB needs.

> **There's a real lack of clarity about who is responsible for securing transactions. The answer is that both business and financial institutions need to do a lot more. This is about risk management, and the current state of play suggests people are too exposed.**
>
> David Emm, Global Research & Analysis Team, Kaspersky Lab

6 Global IT Risks Report 2014: The true cost of data breaches

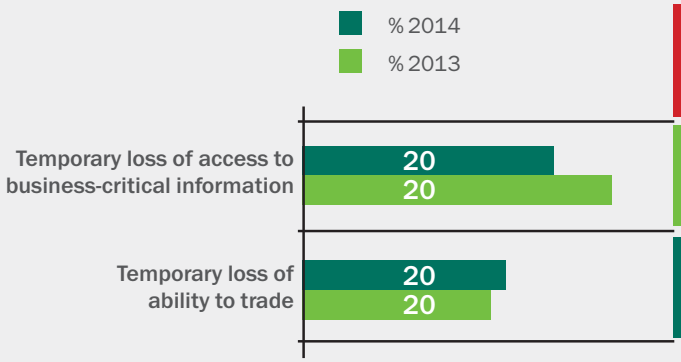
What could a data breach cost your business? If you haven't been through the ordeal, it can be a difficult question to answer. If you have, you'll know all too well the price your business had to pay. The aftermath of a data breach is always more than the initial loss of sensitive and confidential information and the damage it causes goes much further.

Security breaches often result in a number of additional expenses – including remedial and preventative actions. Yes, there's the immediate fear that confidential company information is now in the hands of cybercriminals, but the lasting repercussions can include the cost of data loss, reputational damage, reduced organisational efficiency, third party costs, reactive spending and missed opportunities.

These can be catastrophic for any business. Of the companies surveyed that had experienced a data breach, **55%** found it very difficult to function as they had before. And not just in the short-term. **54%** of companies revealed that data loss had had a negative impact on their reputation, reducing their perceived reliability in the eyes of customers, stakeholders and the wider business world.

The figures below show more about the longevity of disruption that a data breach can cause, as well as the sheer number of businesses that are left without the ability to trade and make money.

IMPACT AMONG THOSE REPORTING EACH EVENT



	Very short term	Short term	Significant	Extended
Temporary loss of access to business-critical information	20	39	31	10
Temporary loss of ability to trade	17	42	30	10

The great majority of businesses – **87%** in fact – were unable to resolve the problem alone, and had to seek help from professional services. These included IT security consultants and lawyers through to auditors and risk management consultancies. Almost half of these businesses (**47%**) said that these services resulted in significant additional costs.

But reactive spending isn't only confined to using third parties. SMBs, if they experience a data breach, could potentially spend up to an additional $7,000 on staffing, $6,000 on training, and $9,000 on systems. And enterprises – larger, but with arguably more at stake – could potentially spend up to an additional $59,000 on staffing, $35,000 on training, and $75,000 on systems.

> **After a security breach, data loss is only the tip of the financial iceberg – the true cost is much greater. There are obvious hard costs such as additional security measures and legal advice, but brand damage and reputation are arguably much larger.**
>
> Costin Raiu, Global Research & Analysis Team, Kaspersky Lab

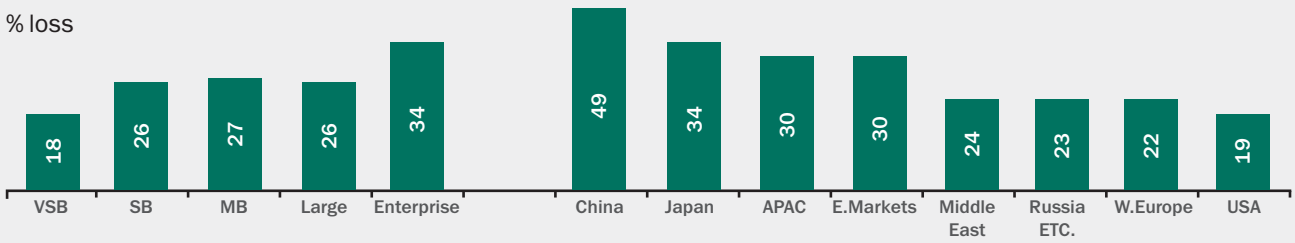
Losing the ability to operate is another major cause for concern after a data breach or security attack. Of the companies who had experienced data loss, about a third were left without the ability to trade. But there is some good news here, between 2013 and 2014, both small and large companies have become better at protecting themselves in this instance, with the average cost of downtime decreasing for both SMBs and enterprises, as illustrated below.

Company size	Cost of downtime	
	2013	2014
SMBs	$64K	$57K
Enterprises	$1.7M	$1.6M

What can businesses learn from these findings? Basically, that reactive spending is always more expensive than proactive spending. So businesses now need to be asking, "Can we afford not to protect ourselves?"

There's an interesting response to this question. On average, a little over a quarter of companies (**26%**) are actually willing to accept a data loss or security breach. Why? Because they perceive it to be less costly than upgrading their IT systems to prevent one in the first place, as we can see below.

"We are willing to bear some financial loss from cybercrime, because it will still be less than the cost of upgrading our IT systems to prevent it."



While we would certainly be interested to see the calculations made to arrive at this conclusion, we don't agree. The potential damage resulting from data breaches extends far beyond the immediate costs. Business continuity, brand equity, reputation and potential third-party costs far outweigh the financial cost of effective, multi-layered threat protection.

7

Global IT Risks Report 2014: The management challenge – in a complicated world we need to make things simpler

This year's survey brought into clear focus the complexity that all sized organisations of all sizes are faced with.

And they're faced with complexity on two fronts:

1. Increasing threat complexity

Malware has very quickly become far more sophisticated. To stay safe, all organisations need deeper protection than a simple 'anti-virus' solution can offer. This has created the perception of having a more burdensome, complex set of tools to manage. And in some cases this perception is justified. The security market is packed with thousands of niche product offerings that under-resourced IT teams struggle to learn, integrate and manage.

2. Increasing IT infrastructure complexity

Even small organisations are powered by a surprisingly complex array of technology. On top of the basic LAN, organisations typically have multiple types of company-wide software, as well as individuals installing 'rogue' applications on their systems. Add to this the growth of virtualization and you have lots of elements to keep track of and manage. But it's mobility that's really posing the biggest challenge to IT professionals.

So, what should IT professionals be doing when the task appears daunting? Here's our list of recommendations:

Manage one unified security system

The challenge we see most often is that when a new task appears (e.g. patching applications) it causes an impulse-buy for a specific solution. While in isolation this is fine, after time it results in a complex array of disconnected systems. In practice, this means more to manage and it creates more work, and opens up new vulnerabilities (as there are too many things to keep an eye on).

Include mobile as part of the bigger plan

Make the assumption that the vast majority of your workforce will have some kind of mobility aspect to their work and you're thinking the right way. Once again, a separate mobile security tool will end up being another thing to manage – and this actually creates new vulnerabilities in your overall IT security.

Recalibrate your approach: invest in multi-layered protection

With the continued rise in the number and sophistication of threats, it's clear that we're underestimating both the scale and the severity of the security challenges we face. Network intrusion, phishing attacks and DDoS are all substantial threats and can lead to very costly data breaches. But the real threat? It's still malware.

Given this, it's now crucial that businesses invest in multi-layered protection. Anti-virus on its own is no longer good enough. Businesses must take a far more proactive approach in managing the behaviour of sophisticated malware that lurks on seemingly safe websites, that appears from seemingly innocent files, that benefits from application vulnerabilities and that take advantage of insecure devices or even unsecured WiFi. The volume of new malware, coupled with its sophistication, makes proactive protection essential, not a 'nice to have'.

Don’t think that fraud won’t happen to you

It’s no surprise that a business’s reputation is important to its customers. What is surprising is that over a quarter of companies surveyed don’t think that banks are doing enough to secure their financial information. Perhaps more surprising still was that 4% of businesses operating some sort of online service took no specific measures to protect their clients.

Never give up on user education

As an IT professional, your job is to ensure you’ve got the right tools and systems in place, and to ensure your staff are educated. Employees can unwittingly allow a security breach and technology can help prevent this to a huge extent. But coupling this with education and real hard-and-fast rules and policies will drastically improve your IT security levels.

There’s a lot to do, but the task is not the impossible one that some people believe.

Meet our Experts

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

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 http://securelist.com/author/costin/ or follow @craiu on Twitter.

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, the human aspects of security and KL technologies. David's blog can be found at http://securelist.com/author/davidemm/ or follow @emm_david on Twitter

Sergey Lozhkin
Senior Security Researcher, Global Research & Analysis Team, Sergey joined Kaspersky Lab in 2012. In his current role he conducts research into cyber espionage, the static and dynamic analysis of malware, Undernet networks such as TOR, social engineering, secure data transfers, exploit analysis, anonymous networks, and cybercrime in general.

Prior to joining Kaspersky Lab, Sergey worked at several companies as a penetration test specialist and virus analyst. He also investigated cybercrimes for the Russian Interior Ministry after graduating from the Omsk Academy of the Ministry of Internal Affairs.
Read his blog at http://securelist.com/author/sergeyl/ or follow @61ack1ynx on Twitter

GET STARTED NOW: FREE 30 DAY TRIAL

Discover how our premium security can protect your business from malware and cybercrime with a no-obligation trial.

Register today to download full product versions and evaluate how successfully they protect your IT infrastructure, endpoints and confidential business data.

GET YOUR FREE TRIAL NOW

JOIN THE CONVERSATION

#securebiz

Watch us on YouTube

View us on Slideshare

Like us on Facebook

Review our blog

Follow us on Twitter

Join us on LinkedIn

Learn more at kaspersky.com/business

ABOUT KASPERSKY LAB

Kaspersky Lab is the world's largest privately held vendor of endpoint protection solutions. The company is ranked among the world's top four vendors of security solutions for endpoint users*. Throughout its more than 17-year history Kaspersky Lab has remained an innovator in IT security and provides effective digital security solutions for large enterprises, SMBs and consumers. Kaspersky Lab, with its holding company registered in the United Kingdom, currently operates in almost 200 countries and territories across the globe, providing protection for over 300 million users worldwide. Learn more at www.kaspersky.com.

* The company was rated fourth in the IDC rating Worldwide Endpoint Security Revenue by Vendor, 2012. The rating was published in the IDC report "Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares (IDC #242618, August 2013). The report ranked software vendors according to earnings from sales of endpoint security solutions in 2012.