Exclusive 2012
Survey Results

Coping in the chaos?

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

Be Ready for What's Next
kaspersky.com/beready

Executive summary

The number, complexity and diversity of cyber threats is soaring. Businesses are increasingly concerned about the risks they face and 91% of organisations have directly experienced at least one cyber threat in the past year. Yet despite evidence of the dangers, Kaspersky Lab's **2012 Global IT Risks Survey** reveals an increasingly chaotic security landscape – where over 40% of businesses feel underprepared for the threats around them.

At the heart of this feeling is a difficulty in mapping awareness into realistic policies and practical security deployments and controls.

- Despite the fact that 35% of organisations have lost business data via malware, a third of respondents have not yet fully implemented anti-malware solutions.
- Although 44% of companies now protect their sensitive data via encryption, 44% place no controls on staff access to network and corporate resources via a notebook and 33% allow uncontrolled access via smartphones.
- Bring your own device is on the increase and usage restrictions are relaxing, particularly on video streaming and website access controls.
- Even social networking and FTP sites are becoming broadly accepted in a growing number of organisations.

Yet at the same time, senior management's awareness of threats is deemed to be increasing and security budgets for the most part are viewed as sufficient.

These seemingly contradictory responses epitomise the findings of Kaspersky's 2012 Global IT Risks Survey. The survey, which polled more than 3,300 senior IT professionals in 22 countries, paints a vivid picture of an increasingly divided security community.

At one end of the spectrum, there are those that recognise the risks and are actively responding to them. At the other end, sit a hard-bitten core of cynics – the 36% of respondents that view most IT security issues as simply unavoidable – and the complacent (32%) who believe that such issues happen to others.

These vastly divergent attitudes to coping in the chaos underline the fact that IT security is a mindset, rather than just a product. With threat levels set to increase further and targeted attacks becoming more common, Kaspersky believes that the outcome will be a growing gap between those that can and do cope, and those who prefer to bury their heads in the sand.

For those seeking to ensure they are protected, Kaspersky offers the following recommendations, discussed in more detail in section 10 of this report:

1. Recognise the nature of the threats you face
2. Be prepared for targeted attacks
3. Develop a consistent and effective policy around mobile and removable devices
4. Introduce data encryption as standard
5. Focus on user education

Contents

Introduction: reality versus perception

1

“This survey comes at a time when the sheer number of threats is higher than ever. But more importantly, the type of threats organisations face has evolved. In particular, the emergence of advanced persistent threats, sufficiently sophisticated to steal data from military contractors and web specialists, changes the rules for businesses.”
Costin Raiu
Director, Global Research and Analysis Team
Kaspersky Lab

In a world ever more dependent on IT for work, play, commerce, finance and everyday communication, it is sadly inevitable that the number and range of threats to IT systems, and both corporate and personal data are higher – and growing faster – than ever. As of September 2011, Kaspersky was tracking over 67 million unique threats; yet it was only in January 2011 that the milestone of 50 million was reached. That equates to a 34% increase in only nine months, or an average of 125,000 unique threats a day.

The diversity of those threats is equally significant. Our research indicates that one in every 14 downloads from browsers now contains malware. But today it is hacking groups and collectives like Anonymous and LulzSec, rather than malware, that have become household names as they carry out pinpoint attacks on company websites. Advanced persistent threats are increasingly commonplace, stealing financial data, intellectual property and commercially sensitive information not only from the corporates and government bodies that are typically their prime targets but also an increasing number of medium-sized and small businesses.

One of the factors in their spread is the increased number of vulnerable endpoints, and in particular a growing reliance on mobile devices, which is putting more companies at risk as these devices are easier to steal or lose, and typically less protected than a desktop infrastructure.

It is perhaps no surprise, therefore, that our second **Global IT Risks Survey** found that – as last year – some 91% of organisations have experienced at least one attack in the preceding 12 months. The focus of the survey is not just the reality, but also the perceived threat to business – and how organisations are responding. It asks about their concerns and priorities and how these have changed; more importantly still, it seeks to understand how they are addressing these issues.

- More than 67m unique threats are now on Kaspersky’s database.
- Threats are increasing by 125,000 a day.
- 1 in 14 downloads contains malware.
- 91% of organisations have experienced at least one threat in the last year.

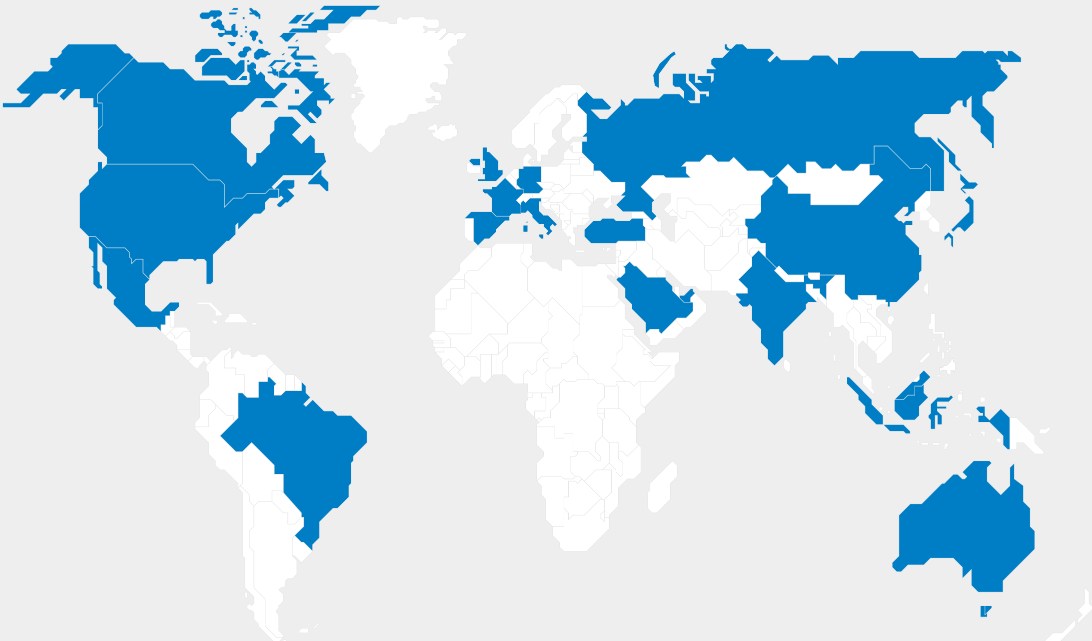
“Effective IT security is always a balance between risk, cost and convenience, but that means you can only evaluate the latter two accurately if you have a full understanding of the former. My concern, which the results of the survey support, is that currently the risks are rising faster than businesses realise.”
Chris Christiansen
IDC – VP Security Products & Services

The survey, conducted by B2B International in July 2012, questioned more than 3,300 senior IT professionals from 22 countries – all of whom have an influence on their organisation’s IT security policy. Respondents represented Small Businesses (SB) with 10-99 seats, Medium Businesses (MB) with 100-999 seats and Enterprise Organisations (E) with 1000+ seats.

What their responses show, overall, is a clear gap between the reality – the growing number of threats – and business perception, or at least business desire to address the dangers out there. While some are adequately prepared, many are not, providing further incentive, if any were needed, for the ever more sophisticated and organised hackers, malware and spyware developers, and spammers.

More than 3,300 senior IT professionals, across 22 countries

Country	No. of respondents
Australia	100
Brazil	201
Canada	100
China	203
France	200
Germany	199
Hong Kong	050
India	200
Indonesia	102
Italy	200
Japan	200
Malaysia	100
Mexico	109
Middle East (Saudi Arabia & UAE)	201
Russia	361
Singapore	051
Spain	200
Taiwan	050
Turkey	100
UK	200
USA	200



Cyber threats are recognised as a major risk to business

2

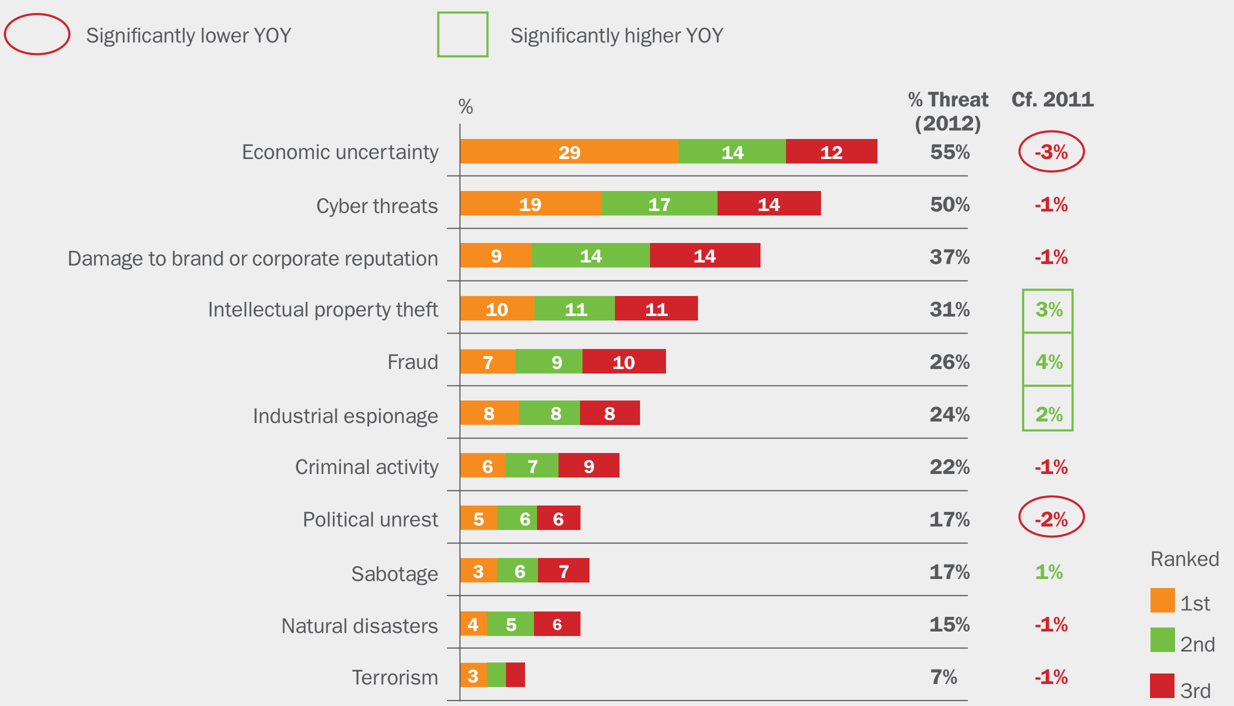
Half of the organisations in our survey see cyber threats as one of the three most critical risks to their business: 19% see them as the single greatest risk. Perhaps not surprisingly, the only risk that ranks above cyber threats in our survey is the ongoing economic uncertainty.

While the number of organisations ranking cyber threats as one of the top three risks has dropped marginally (1%) compared to 2011, it remains comfortably ahead of the third biggest risk, damage to brand or corporate reputation – itself often a consequence of a major outage, virus attack or data loss.

What's more, several other related issues – such as intellectual property theft, fraud and industrial espionage, all of which are now increasingly likely to occur via hacking, malware or spyware – are all seen as growing risks over the last year.

Top current business risks

50% of businesses see cyber threats as a critical risk to their organisation



“Despite empirical evidence that the number of threats is growing, only half of organisations perceive an increase. For some people a certain threshold has been reached above which anything extra is just noise.”
Roel Schouwenberg
Senior Security Researcher
Kaspersky Lab

“One clear trend from the data is that companies are becoming aware of the changing threat landscape and the fact that malware is being used for more than just theft of money.”
David Emm
Senior Regional Researcher
Kaspersky Lab

This is perhaps one reason why over half (52%) of respondents perceive that the number of cyber attacks against organisations has increased over the last 12 months – on the back of 49% perceiving a rise the previous year.

The expectation is that this trend will continue: 42% agree that cyber threats will be much more of a concern in two years' time – putting it top of the rankings, ahead of economic uncertainty. Given this ongoing rise in threat levels and impact, it would seem imperative that organisations act now to ensure they are adequately prepared.

Small businesses are increasingly conscious of increased cyber threats:

- 47% believe attacks are increasing, up 2% on 2011.
- 52% of all respondents are worried about the involvement of criminal gangs in cyber attacks.
- 42% are concerned about increased Government interference – up on 2011.

Underprepared and under-resourced: how organisations view their readiness for cyber threats

3

“The fact that most businesses feel that they are well accounted for when it comes to a cyber attack is a false perception. Many organisations do not know what they are actually protecting, or what the worst case scenario is for their organisation.”
David Jacoby
Senior Security Researcher
Kaspersky Lab

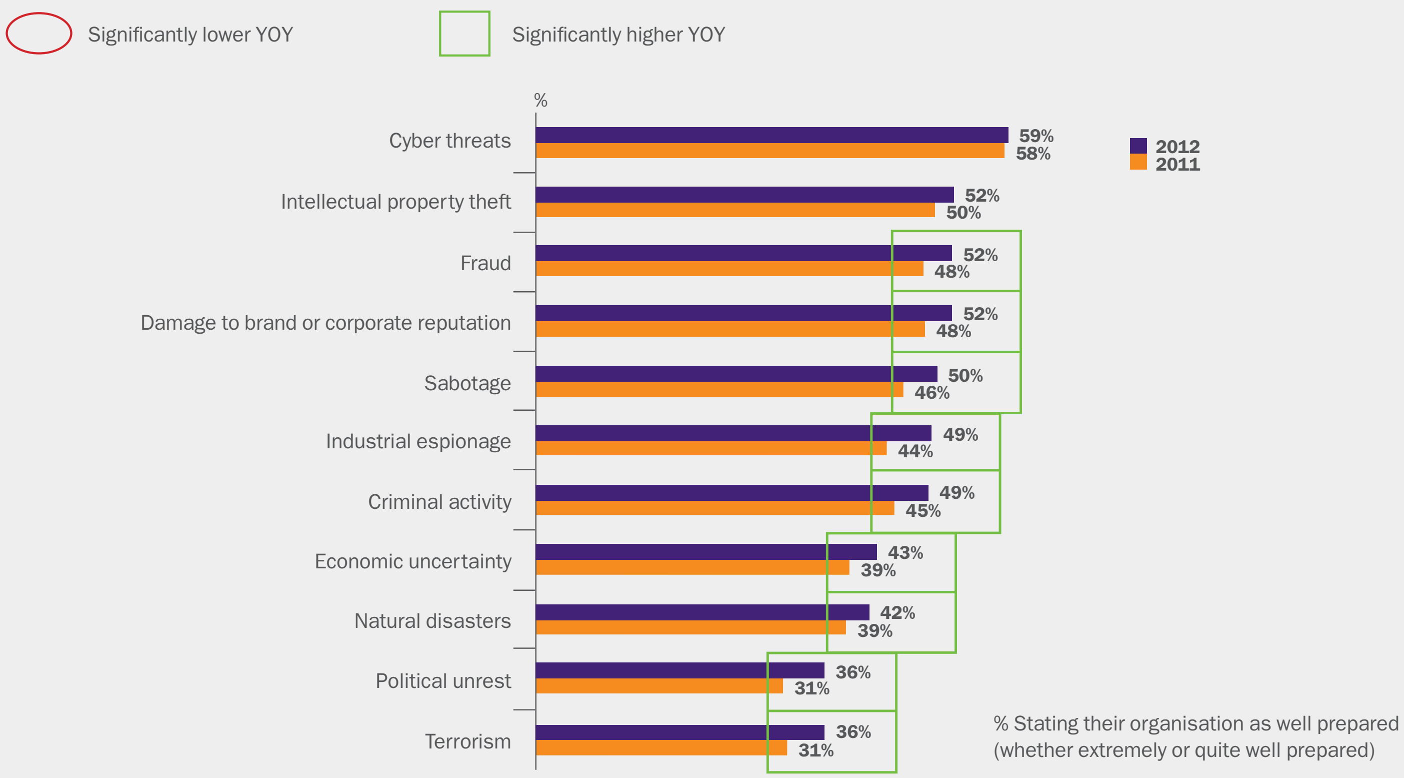
Despite the recognition of the growing danger of cyber threats, 41% of organisations in our survey do not feel well prepared for the coming wave. While 59% of organisations are confident they have accounted adequately for cyber threats, this is an increase of just 1% from 2011’s figure – a slower increase in readiness than for any other risk.

This is inspite of the fact that preventing IT security breaches remains the number one concern of IT professionals – and the fact that cyber attacks are more predictable and preventable than natural disasters and economic uncertainty. A 2012 study by Verizon found that 97% of attacks could have been avoided with ‘basic or intermediate’ security controls.[1]

This year’s survey shows important increases in preparation for the related issues of intellectual property (IP) theft, fraud and industrial espionage. While this indicates a growing understanding of the full range of technology related risks, approximately half of all organisations describe themselves as well-prepared against these specific threats.

[1]2012 Data Breach Investigations Report Verizon Business, 2012

Preparation for different business risks



“People will feel more confident about some things than others. They may feel confident about fending off mass malware attacks, but not so much about a targeted attack.”
Roel Schouwenberg
Senior Security Researcher
Kaspersky Lab

One key factor in this sense of being underprepared may be financial: 41% believe their organisation’s current level of investment in IT security is inadequate. While this shows a 5% increase in the number of organisations that believe they are adequately resourced compared to 2011, there remains a considerable gap between perception of risk and business willingness to respond. The public sector is particularly under-resourced: 53% of respondents there feel their security budget is too low.

There is also an unanswered – and perhaps unanswerable – question about what ‘adequate’ preparation for any risk is. The growing number of zero-day attacks, where cyber criminals take advantage of security vulnerabilities in software before the vendor has even realised they exist, is testimony to the challenge of putting in place adequate preparation: if you do not know what the risks are, how can you prepare?

- 31% of respondents said preventing IT security breaches is their IT team’s number one priority; 27% said data protection.
- Median spend per employee on IT security is $138 in enterprises, $50 in medium-sized businesses and $34 in small businesses.
- 58% of respondents said their IT security was under-resourced in at least one area of staff, systems or knowledge.

Fewer organisations have fully implemented anti-malware

4

“Most people view anti-malware as the one-stop solution that fixes all problems – which is why it is the area most commonly identified as needing to improve. But important as it is, pure anti-malware can’t solve everything: security is a mindset, not a product.”
Roel Schouwenberg
Senior Security Researcher
Kaspersky Lab

In most people’s eyes, anti-malware solutions are a fundamental component of a security strategy – and it is the most commonly implemented measure taken to avert security risks. But even here, only two-thirds of respondents claim to have fully implemented anti-malware, a figure that is 5% lower than in 2011.

What’s more, there is only a marginal difference between organisation types: 67% of small businesses have fully implemented anti-malware, compared to 66% of medium-sized businesses and 70% of enterprises. Given that 35% of organisations acknowledge they lost business data via malware (14% of whom have reported losing sensitive data) and anti-malware is seen as the most effective measure against information security threats, this trend is alarming.

Measures taken to avert security risks

Significantly lower YOY

Significantly higher YOY

Measure	%	Cf. 2011
Anti-Malware protection (Anti-virus, Anti-spyware)	67%	-5%
Regular patch/software update management	62%	0%
Implementing levels of access to different IT systems by privilege	45%	0%
Network structures (e.g. separation of mission-critical networks from other networks)	45%	3%
Encryption of highly sensitive data	44%	7%
Physical security of critical IT systems (e.g. prevention of theft, fire-proofing)	43%	1%
Disaster recovery policy and preparation	42%	4%
Separate security policy for removable devices (e.g. USB’s)	38%	N/A
Policy for dealing with IT security at remote branches/offices	37%	2%
Separate security policy for notebooks/laptops	36%	N/A
Encryption of all stored data (i.e. full-disk encryption)	36%	N/A
Encryption of business communications	34%	3%
Auditing/verifying the IT security of third party suppliers	33%	2%
Separate security policy for smartphones/tablets	32%	N/A
Encryption of data on removable devices (e.g. USB’s)	32%	N/A
Client Management (PC Lifecycle Management)	32%	N/A
Mobile device management	23%	N/A

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

“Perhaps their chosen vendor only provides limited support, for example they have nothing for Blackberry devices. Or because there is no way of protecting them like the iPhone, because the OS is locked down.”
David Emm
Senior Regional Researcher
Kaspersky Lab

One possible explanation is that the key word in the question is ‘fully’. Fully implementing anti-malware is increasingly difficult as device usage evolves, particularly around smartphones. Perhaps their chosen vendor only provides limited support, for example they have nothing for Blackberry devices. Or because there is no way of protecting them like the iPhone, because the OS is locked down.

Given these risks, and as usage of mobile devices soars both for email and access to corporate data and applications, it may be time to revisit mobile usage policy. Currently only 32% cite a separate security policy for smartphones and tablets, and 22% use some form of mobile device management (MDM) – with a sizeable difference between enterprises where 31% have implemented MDM compared to just 17% in small businesses.

- Anti-malware protection was rated the most effective measure against information security threats, receiving an average rating of 3.7 out of 5.
- All measures received an average score of 3.2 or higher.
- Only two measures are fully implemented by more than 50% of organisations: anti-malware and regular patch management.
- Over half of enterprises have also implemented different levels of access to systems, separation of network structures, investments in physical security and sensitive data encryption.

Use of encryption is growing

5

“The rise in encryption is directly related to the growing realisation that ‘always-on’ staff, working any time, any place, anywhere and from any device, puts unencrypted data at greater risk than ever.”
David Emm
Senior Regional Researcher
Kaspersky Lab

One clear trend across the survey is a growing use of encryption, particularly at enterprise level. 44% of organisations now encrypt sensitive data – up 7% on 2011 survey results – and 34% encrypt business communications, a 3% increase over 2011. 36% use full disk encryption and 32% have implemented encryption of data on removable devices.

Encryption is a measure designed to minimise the impact of security breaches, rather than necessarily prevent them, and its rise perhaps reflects the growing diversity of threats, such as the theft of intellectual property (IP) and industrial espionage. If encrypted, stolen data is of no value to the thief. Another potential reason for the increased use of encryption technology is the fact that more data is now carried around off-premise, on smartphones, notebooks and removable storage – all of which can be easily lost or stolen. Encryption is a way to reduce the risk, rather than seeking to curb or change the behaviour.

Use of data encryption

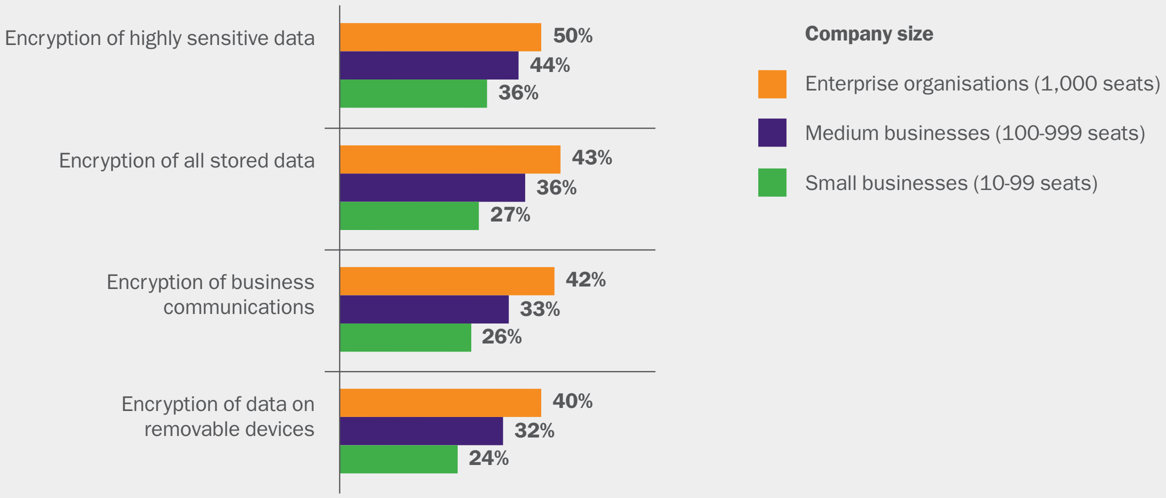


Chart shows % of organisations that have **fully** implemented data encryption

“The fact that encryption for removable media remains under-used suggests that a lot of people don’t take the threat here seriously – as if they can’t imagine putting highly sensitive data on (unencrypted) removable storage. Yet time and again, that’s exactly what happens.”
Roel Schouwenberg
Senior Security Researcher
Kaspersky Lab

But encryption is often perceived as a complex and costly solution, which perhaps explains the distinct gap between its usage at enterprise level and in smaller organisations. 43% of enterprises encrypt all their data, but only 36% of small businesses encrypt highly sensitive data.

While the efficacy of encryption is increasing, it is also an area where respondents would like to see improvements: encryption of sensitive data ranked second as the area most organisations would like to improve.

- Loss of sensitive data in Global Cooperation Council (GCC) countries has increased by 14%, by 6% in Europe and 9% in Commonwealth of Independent States (CIS).
- 15% of organisations have experienced data loss as a result of theft of mobile devices.
- 9% have lost data due to corporate espionage.
- Malware and spam remain the biggest causes of data loss – though both decreased in 2011.

Bring your own device has emerged as a key challenge

6

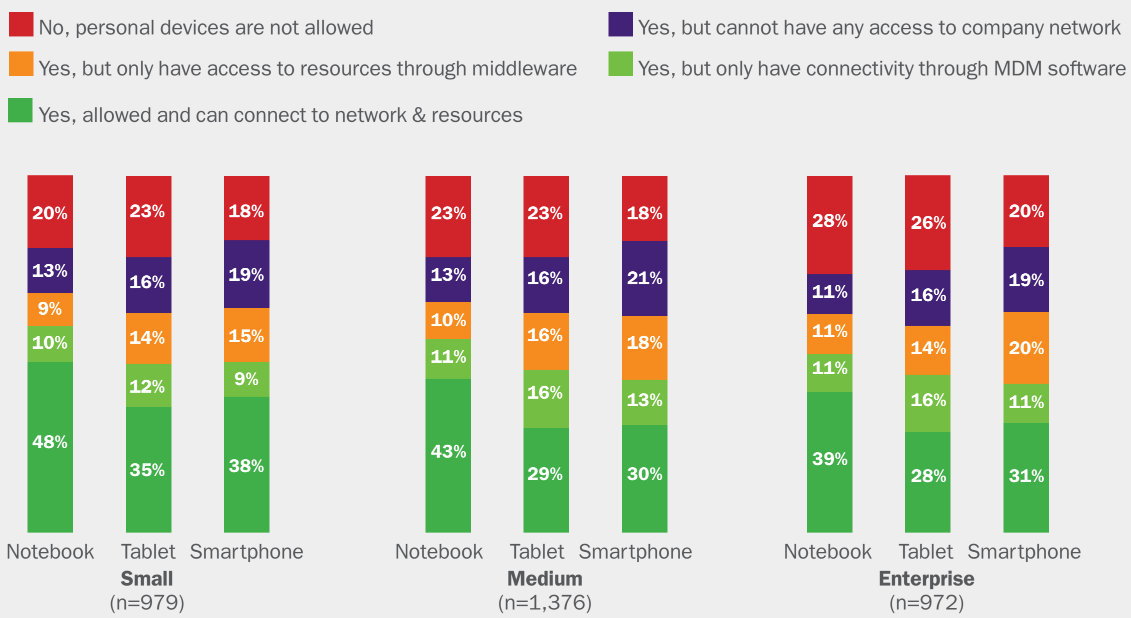
"BYOD is one of the biggest risks to IT security. Both in targeted and non-targeted attacks having personal devices on the network brings extremely difficult challenges. Ideally, personal and business use should be completely separated and segregated."
Roel Schouwenberg
Senior Security Researcher
Kaspersky Lab

Last year's survey highlighted a challenge to IT security caused by the rapid increase in the numbers and types of devices connected to the corporate network. In the last year, a further challenge has emerged: the concept of 'bring your own device' (BYOD). 44% of companies allow staff uncontrolled connectivity to the network and corporate resources via a notebook; 33% permit this via smartphone.

The logic behind the approach is two-fold: it enables users to work the way they want – therefore driving productivity – and means businesses can reduce the costs of device purchases. But from the security perspective, it is fraught with risk. Enforcing a corporate security policy is far more complex when employees own their devices: whilst restrictions may be in place when users are on the corporate network, in their own time employees are able to use their device to access any content or sites they wish, potentially bringing a threat into the business. There are also legal and privacy concerns around issues such as installing corporate software on personal devices, and remotely wiping data if the device is lost or stolen – or simply if the employee leaves the company.

Yet across all sizes of organisation – even enterprise – BYOD policies are surprisingly liberal. While some insist on access via middleware or mobile device management software, very few have banned personal smartphones altogether. That's despite the fact that many enterprises will provide their staff with a corporate smartphone.

Own device usage



“The up-front convenience and cost-saving of BYOD is attractive, particularly for small and medium businesses. But BYOD presupposes a mixed environment, which actually increases the cost and effort of managing mobile devices within the overall corporate security strategy.”
David Emm
Senior Regional Researcher
Kaspersky Lab

What’s more, the majority of organisations believe that personal device usage is a growing trend, and have few plans to restrict it in the future. Indeed, 36% state that they will actively encourage BYOD, while a further 36% see its increase as inevitable. In such an environment, device control would seem to be essential: instead of operating a number of device-specific solutions, a centralised, independent device control platform that manages the overall device policy – and any necessary restrictions – is a more flexible and secure option.

- Just 12% of enterprises plan to enforce a strict prohibition on own device usage for work purposes.
- Overall, tablets are currently the most restricted devices.
- Access through middleware is the most common approach to limiting own device usage.

Restrictions on user activities are decreasing as their business value becomes clear

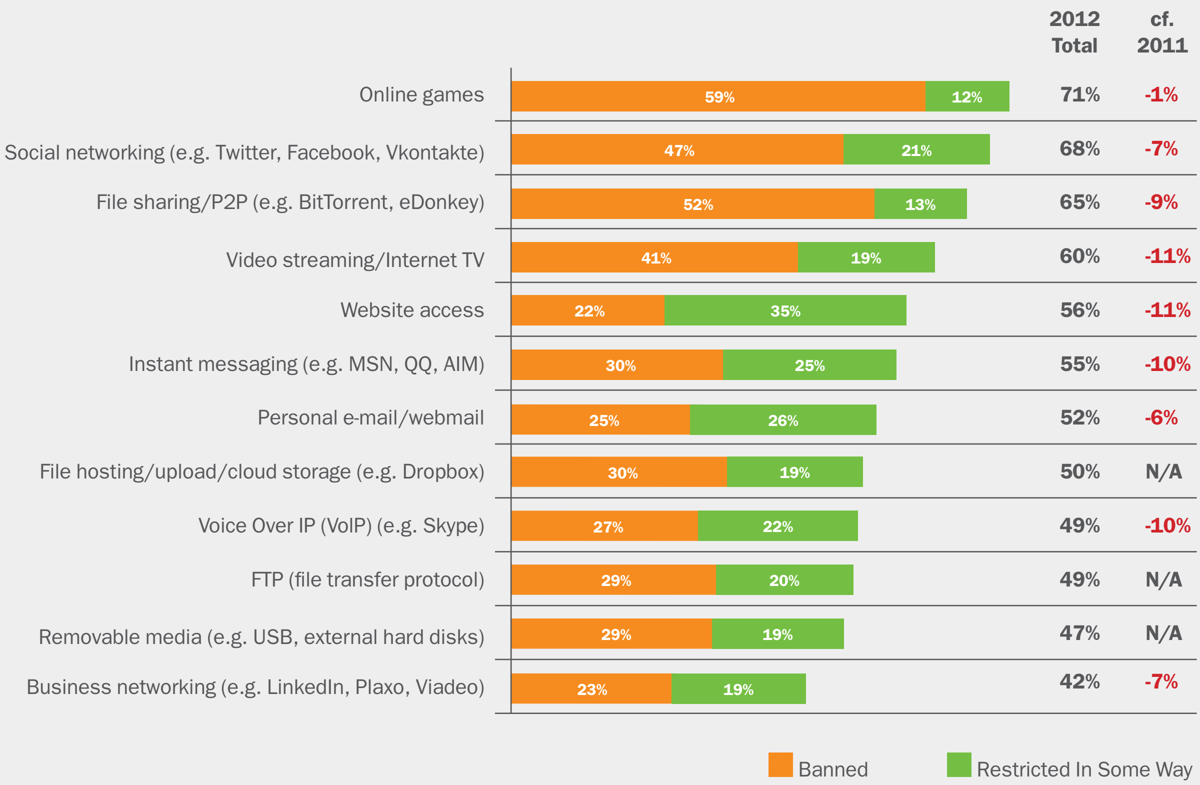
7

"To outlaw use of social media across the board would be akin to trying to turn back the tide: far better to work out how to manage it."
David Emm
Senior Regional Researcher
Kaspersky Lab

In line with this sense of growing permissiveness, the survey revealed a significant decrease in restrictions on usage – with a drop in every category where comparative data was available. The biggest decreases in restrictions were around video streaming (11%), website access (11%), instant messaging (10%) and voice over IP (VoIP) (10%).

The prime reason behind this is undoubtedly that businesses are seeing the potential value of these activities: more and more companies use some form of instant messaging for internal communications. VoIP solutions offer immediate cost savings, yet embracing these technologies opens up new vulnerabilities. Peer to peer applications expose endpoints: something as simple as saving a private file to a shared drive can then enable unauthorised access to sensitive information. Innocent-looking instant messages can contain links that, when clicked, download malware.

Banned/restricted activities



“I still don’t understand why social networking is viewed as a high threat when FTP or file hosting and upload are seen as ‘legitimate and safe’, I would say the opposite. The only reason I would block social networks would be if employees spent all their time on them rather than doing work.”
David Jacoby
Senior Security Researcher
Kaspersky Lab

But when it comes to user restriction, the hottest topic is undoubtedly social networking. It is seen as one of the highest threats to IT security, and remains the second most closely-controlled, with just under half of organisations banning it outright. This is marginally down from 2011, reflecting both the sheer ubiquity of social networking, and an increased acceptance that it offers business value.

One important factor to bear in mind here is that the risks associated with social networking are – in general – the third-party applications, rather than the sites themselves: users clicking on adware and surveys embedded on social media sites may be inadvertently opening new dangers. Instead of comprehensive restrictions, this suggests a better approach may lie in increased application control that can disable risky add-on applications and features.

There is also a sense that focusing on social networking can leave the business blind to other dangers. For example, the survey found that activities such as file hosting/uploading and FTP are seen by the majority as ‘largely legitimate and safe’, perhaps due to a lack of high-profile attacks. Yet evidence shows that when using FTP, businesses send their credentials – eagerly sought by cyber-criminals – in clear text nine times out of ten.

The bottom line is that every business will want to use different applications, and with users owning multiple devices, blanket bans are increasingly impractical. Instead, a more granular approach is needed, combining restrictions with user guidance and education, and above all endpoint controls that protects the business.

- Restrictions on social networking use are strictest in Russia and other parts of the CIS, where 79% of respondents have some restriction in place and 61% ban it.
- The least restricted region is North America, where restrictions apply in 62% of organisations.
- In Asia/Oceania and the Middle East, just 42% organisations ban social networking altogether.

Resigned, complacent: a shift in attitudes puts businesses at risk

8

"A lot of organisations think that they have everything under control because they have several functions in place, and that they are following some models to become compliant. But IT security is not only about having systems in place, but also focusing on employee awareness and education, placing reasonable and enforceable restrictions on what they can do, and monitoring vigilantly."
David Jacoby
Senior Security Researcher
Kaspersky Lab

The survey has revealed some serious gaps in security policy – as well as underlining the fact that vast numbers of businesses have felt the impact of cyber threats. 91% acknowledge they have been the victim of an incident in the last year, and 35% have experienced severe data loss. But despite this strong evidence of the risks, 53% of respondents describe themselves as 'highly organised' and 'systematic' in dealing with threats.

More alarming still are two clear attitude shifts over the last year: a 5% increase in the proportion of organisations that believe 'most IT security issues are because of unforeseeable events' and a 6% rise in the number that describe security issues as 'things that happen to others.'

Overall attitudes to IT security

Significantly lower YOY

Significantly higher YOY

	Overall	Emerging	Developed	GCC/ Middle East	LATAM	Asia & Oceania	N. America	Europe	CIS
Base	**3,327**	**1,728**	**1,599**	**201**	**310**	**1,056**	**300**	**1,099**	**361**
We are highly organised and systematic in dealing with threats to our company's computer systems	**53%**	56%	50%	43%	53%	58%	49%	52%	53%
Most IT security issues are because of unforeseeable events - there is no point trying to cover every last possibility	**36%**	41%	29%	36%	38%	42%	23%	33%	33%
Security issues are things that happen to other organisations - we have never encountered any problems ourselves	**32%**	36%	27%	35%	28%	38%	24%	30%	27%
Average agreement (across all issues)	**40%**	**44%**	**35%**	**38%**	**40%**	**46%**	**32%**	**38%**	**38%**

“This data is frankly scary. Some would call it a ‘ticking time-bomb’, but I think it’s worse than that. With the time-bomb you eventually see the results. In the case of modern malware, you may never know you’ve been attacked.”
David Emm
Senior Regional Researcher
Kaspersky Lab

Both attitudes ignore the hard evidence. A resigned approach overlooks the reality that incidents such as theft and loss of devices are commonplace but can be protected against; that intentional leaks and fraud are both seen as key internal threats to security and – most curiously of all – that over a third of organisations believe they are now being, or at risk of being, specifically targeted by cyber attacks.

The complacency witnessed sits in direct contrast to the fact that over nine out of ten organisations have been the victim of an attack: in the words of Kaspersky Lab’s Roel Schouwenberg, “There’s a saying now that there are two types of companies. The first is the type of company which has been compromised; the second is a company that simply doesn’t yet know it has been compromised.”

- 10% of organisations strongly agree that most IT security issues are due to unforeseeable events.
- Asia and Oceania is the region where complacency is highest; North America is where it is lowest.
- Developed countries are less confident overall than emerging countries, and the gap is growing.

Bridging the gap: it is now time to act

9

"At a time when senior management commitment to security is rising, it should be an opportunity for security professionals to drive improved policies and invest in priority technologies such as endpoint control. But unless they recognise the real threats they're facing – such as the danger of targeted attacks – those policies will be of limited value."
Costin Raiu
Director, Global Research and Analysis Team
Kaspersky Lab

"As well as the gaps in knowledge and readiness, in many organisations there are also clear gaps on the operational level, with different security solutions and policies applied to different user groups and devices. Every one of those gaps is a potential vulnerability; organisations need to take a holistic approach and look at integrated control solutions."
Chris Christiansen
IDC – VP Security Products & Services

As the survey has shown, there is a substantial gap between reality – a rapidly growing and evolving threat environment – and organisations' perceptions of the dangers they are in. There is a substantial gap between the acknowledged threats, and a readiness to act on them. Above all, there is now a clear gap emerging between those that are well-informed and well-protected, and those that are not.

For example, despite the confidence that many businesses are now 'highly organised and systematic in dealing with threats', almost a third of respondents had not heard of some of the most common cyber threats of the last year. While 33% said they felt their organisation was being or had been deliberately targeted, only 11% believe that such attacks will become a major concern.

But what the survey also showed was that the opportunity to bridge this gap has never been greater. The importance of senior management commitment to IT security is rising, up from 65% in 2011 to 69% in 2012. Security staffing resources are seen as sufficient by over two-thirds of respondents. A growing number even feel that their total security budget is broadly right, even if the way it is allocated might not be.

The key to moving forward therefore may lie not in additional expenditure, but instead better use of existing resources – and in particular around increasing knowledge both amongst IT staff and the user base. With so many threats associated with changing working practices, most notably mobile computing, more rigorous policies and better enforcement – backed by technologies such as device, application and web control – can help to mitigate or even nullify many of the risks.

It comes back to a guiding principle of Kaspersky's work: that security is a mindset, not a product. In responding to the challenges and threats that today's organisations face, getting the mindset right is undoubtedly the first step.

Recommendations

10

So what is the right mindset for dealing with today's complex threat landscape? And once the mindset is in place, what actions should organisations prioritise? Kaspersky Labs' team offers the following recommendations.

1. Recognise the nature of the threats you face
While worms, Trojans, phishing and scanning remain considerable risks, smart organisations have already taken key steps here. Ongoing vigilance remains essential, but organisations in this position now need to take stock of the emerging challenge of advanced persistent threats: harder to detect, harder to prevent and harder to remove. Often moving by stealth, advanced persistent threats can establish multiple backdoors on systems that may even remain inactive for some time. Organisations are not helpless in the face of these, but they must be prepared to take significant action.

2. Be prepared for targeted attacks
Organisations in our survey recognised the growing risk of targeted attacks, and acknowledged they themselves are potential targets. But here again there's a mindset shift needed. In a targeted attack, instead of trying multiple organisations and exploiting the first weakness it encounters, your attacker is focused solely on getting into your infrastructure, your data and your business. This means it is no longer good enough to be safer than your peers: you need to be safe in an absolute sense. Proactive protection, particularly around endpoints, is a must.

3. Develop a consistent and effective policy around mobile and removable devices
From smartphones to removable storage, the number of devices used by employees to access corporate resources is growing at a phenomenal rate, and as our survey showed an increasing number of organisations are embracing 'bring your own device'. It seems unlikely security professionals can resist this trend, so the challenge now is to develop a policy – underpinned by effective endpoint control solutions – that gives users the flexibility they expect but at the same time provides the business the protection it needs.

4. Introduce data encryption as standard
There are many ways in which corporate data can be stolen, leaked or lost – from spyware to accidentally leaving a device on a train – and the risks are growing. To minimise the impact of data loss, we now strongly recommend encryption of sensitive information (or better still, all information). Quite simply, it means that when the almost inevitable occurs, the business is less likely to be damaged.

5. Focus on education
If IT security professionals continue to underestimate the threats they face, it is no surprise that the majority of staff are at best ignorant, and at worst blasé, about the dangers to the business. Organisations must continue to invest in staff training and information, explaining the changed threat landscape and the extra risks that come with using mobile devices, social networking, IM and other tools now seen as standard. This is particularly important as blanket approaches such as barring access to certain sites and tools is increasingly difficult. Users need to understand the threats to the organisation, and what they can do to minimise them.

Be ready with Kaspersky

11

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 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/beready

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 leader 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.

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

David Jacoby
David joined Kaspersky Lab in 2010 as a Senior Security Researcher for the Nordic region. David specialises in UNIX, Linux and web security. His research focuses on improving awareness of the threats to which Internet users are exposed. Prior to joining Kaspersky Lab, David worked in vulnerability research and vulnerability management. He blogs at www.securelist.com/en/blog?author=4346

Roel Schouwenberg
Since 2008, Roel has been Kaspersky Lab's Senior Security Researcher, Americas. Roel specialises in the improvement of proactive detection capabilities and researching the vulnerabilities of many different types of file formats. He is a founder member of the Anti-Malware Testing Standards Organisation (AMTSO) and currently serves as part of AMTSO's Board of Directors. His blog is at www.securelist.com/en/blog?author=64

Kaspersky Lab is also grateful to **Chris Christiansen, IDC – VP Security Products & Services**, for his input. Chris is an acknowledged global authority on a range of security topics, and a regular speaker and media commentator. Keep up to date with Chris's thinking via Twitter.com/cchristiansen.