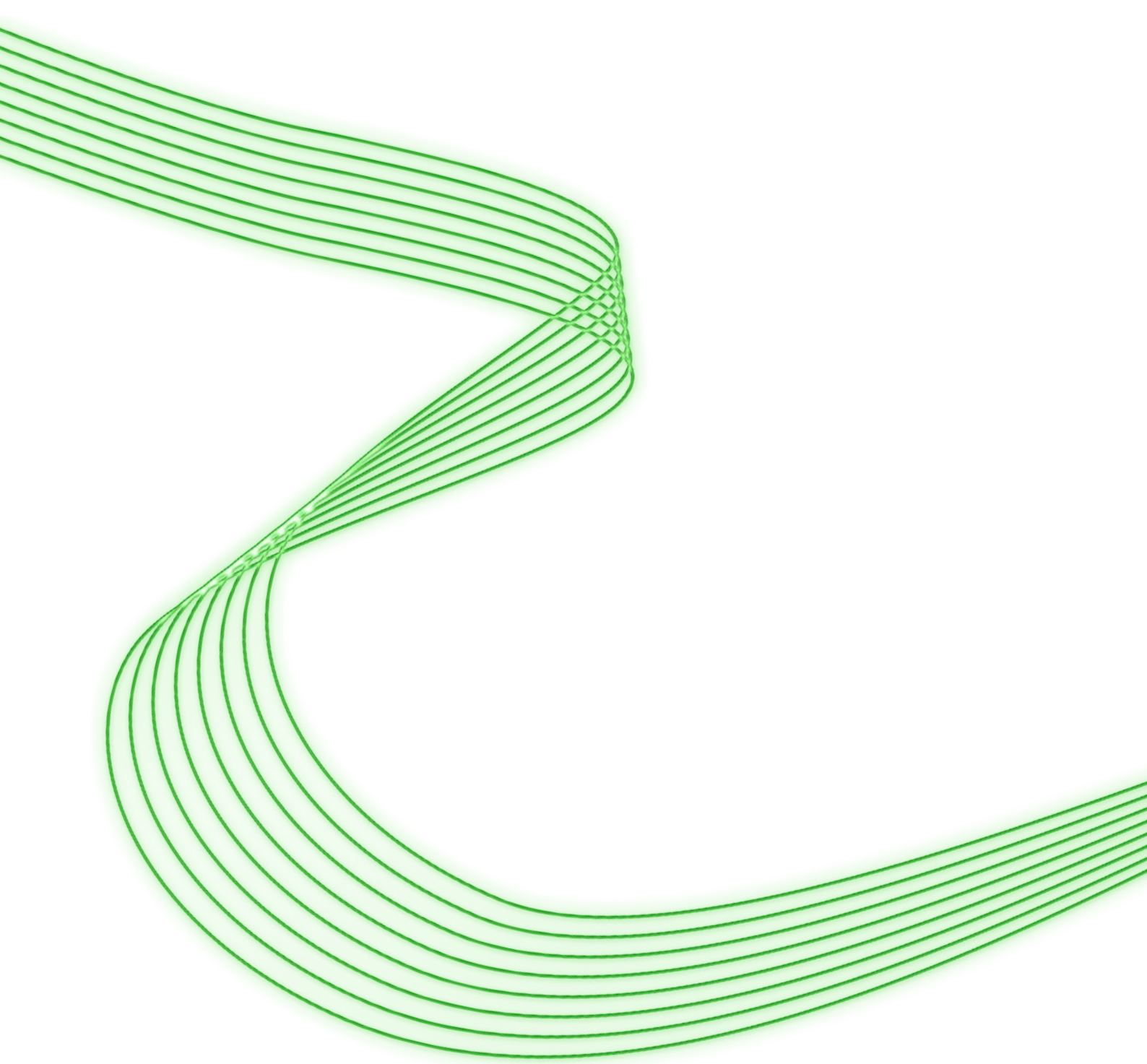


WHY COMPLEXITY IS IT SECURITY'S WORST ENEMY.

A whitepaper analysing how complexity is causing new security challenges, and how best to address this.

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

Be Ready for What's Next

KASPERSKY lab

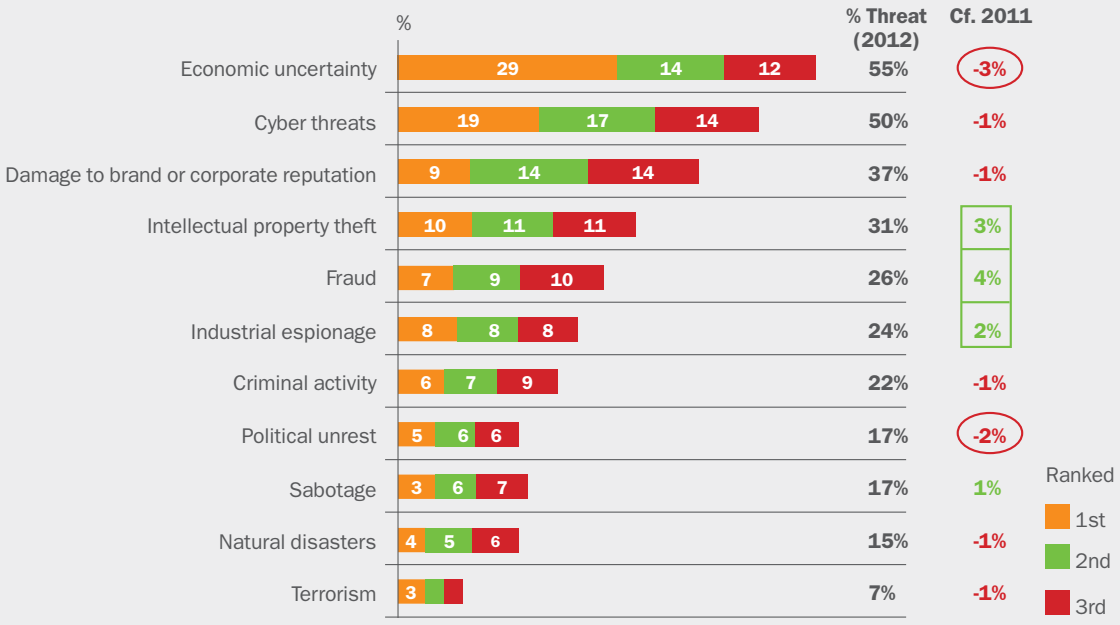
Executive summary

1.0

Organisations across the world continue to strive for greater agility, efficiency and innovation. But they also need to cut costs, improve productivity and become more competitive. While this is nothing new, the fact remains that IT is arguably the key department tasked with supporting these needs and ultimately making this happen.

These new requirements create complexity and extra tasks for IT to manage. But with greater complexity it is easy to miss a system vulnerability such as an unpatched application or new device on the network, which in turn can cause major security issues. Businesses recognise this challenge, and when Kaspersky Lab gathered the opinions and experiences of more than 3,300 senior IT professionals across 22 countries in the **2012 Global IT Risk Survey**, it was no surprise that cyber threats were seen as the second biggest business risk after economic uncertainty (see Figure 1).

Figure 1: Top current business risks[1]



The main technology areas that require extra resource and management tools are mobile, encryption, control features (such as application, web and device control) and systems management: with the often manual task of updating patches ranking top of concerns in the Kaspersky 2012 Global IT Risk survey (see Figure 2).

1 Source: Kaspersky 2012 Global IT Risk Survey

"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."
IDC's VP Security Products & Services, Chris Christiansen[3]

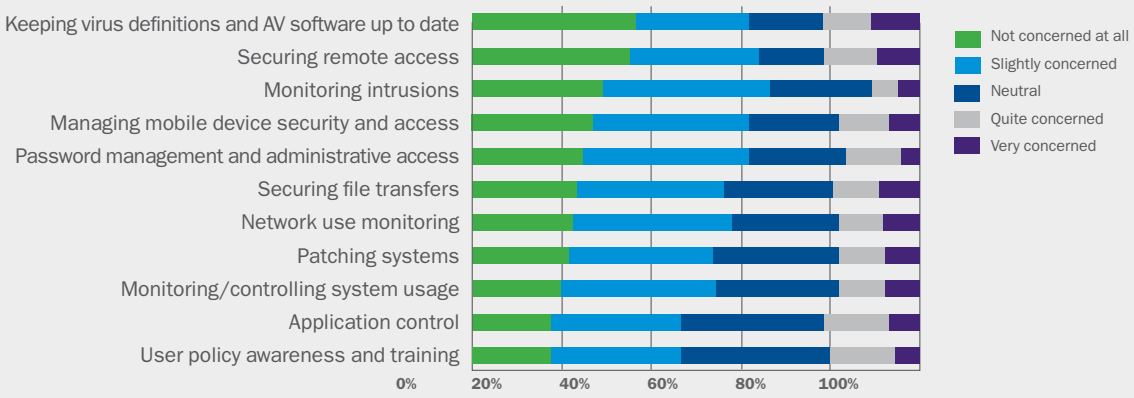
Current IT security solutions can exacerbate the problems associated with complexity as they are typically 'point solutions' for specific issues, such as mobile device management or encryption. At best, they are 'connected', at worse they simply don't talk to each other. This means IT administrators have to jump from one dashboard to another to implement policies, check endpoint status and patch applications. As a result, security gaps can easily occur.

A large global organisation can invest in large 'enterprise-scale' technologies, with dedicated and specialist resource to ensure water-tight IT security. However, this is simply not an option for most SMB organisations, who have to address similar challenges but with a much smaller IT team.

Organisations are caught between competing issues: ever more business-critical data, managing a more complex environment, and external risk factors continuing to expand.

This fact was brought into sharp focus in Kaspersky's 2012 Global IT Risk Survey.[2] On analysing the survey results, IDC's VP Security Products & Services, Chris Christiansen commented *"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."*

Figure 2: How concerned are you about the following IT security challenges within your organisation on a day-to-day basis?[2]



For organisations, who are aware of what needs to be covered (and indeed 'how to cover it'), a new approach is required. One that breaks through existing norms and constraints – and allows resource-challenged IT teams to build and manage a far more extensive IT security posture.

This whitepaper looks at the real challenges faced by organisations, and what new IT security threats and issues have arisen as a result. Increasingly, anti-malware alone is not enough, so this whitepaper investigates what new IT security approach is required to effectively respond to the changing threat landscape and new ways of working.

2 Source: Kaspersky 2012 Global IT Risk Survey
3 Source: Kaspersky Global IT Risk Report 2012

Business drivers: what's creating the challenge?

2.0

The need for a new approach to IT security comes from the changes driven down to IT teams by their organisations. Some of these arise from technology requirements, but all ultimately stem from fundamental drivers for lowering cost, providing greater agility and improving productivity.

2.1 Technology
Technology drives business more than ever before, and this has led to more and more systems and platforms – which we depend on to work effectively. Businesses of all sizes are adopting technologies at a rapid pace and in many different fields of specialisation. Collaboration tools are being embraced – to speed decision-making and cut travel time and cost and organisations are providing a range of mobile devices to employees.

All of this generates ever more data and creates a new generation of 'endpoints' and potential open doors for cyber criminals.

2.2 Under-prepared, under-resourced?
The burden for managing this falls to the IT teams who have a far greater and complex job to do, but often with the same or less resource.

IT managers and administrators wear multiple hats. They have to multi-task, and quickly learn new technologies, in the morning they could be resetting servers, by lunch they're adjusting firewall rule sets and access control lists. In the afternoon, they're walking through mobile device configuration settings so the CEO's new smartphone or tablet can receive email and access the network. And before close of business, they're resolving network address translation conflicts on edge routers. All of this could be seen as just 'business-as-usual', but the challenge comes when you map this activity against the raft of new technologies and requirements that simply didn't exist a few years ago.

2.3 Changing work patterns
Employees are now accustomed to having highly user-friendly and functional technology at their fingertips. This new generation is quick to find collaboration tools, applications and devices and then use them in a business environment.

They're used to accessing web services from anywhere; and having the applications, information and resources they need, in the palm of their hands – often without IT support, or more importantly, without IT mandating how they work or what they work with. This has created a relentless demand for business agility, a side-effect of the 'consumerisation' of technology, which makes it hard to meet expectations in the traditional 'corporate' way of delivering IT.

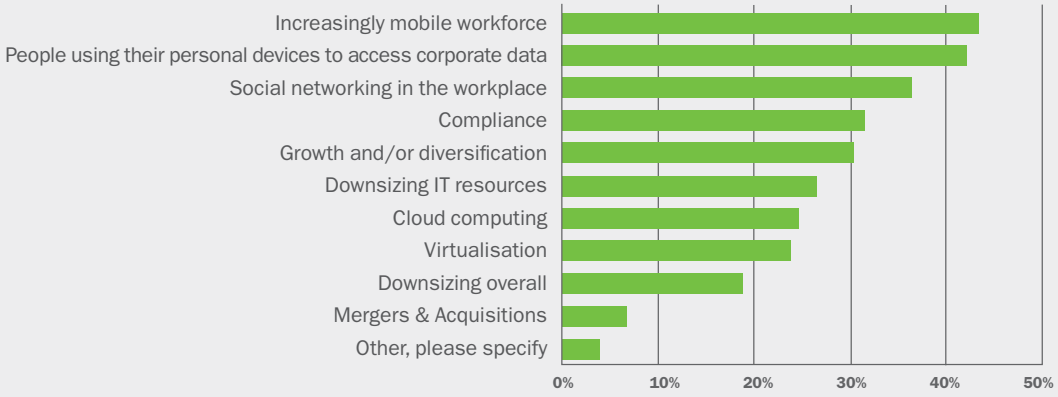
Rather than trying to prevent BYOD, the focus now is to find a way of managing it.

2.4 Mobility

In Q3 2012, IDC reported that 444.5 million smartphones were shipped worldwide, growing by 2.4% year on year.[4] Many of these mobile devices are finding their way into work environments and end users are looking to mobility as a means of blending their professional and personal digital lives.

In March 2012, Kaspersky conducted a piece of global research in conjunction with analysts Bathwick Group **'Security readiness in a changing technology landscape' (see Figure 3)**, which found that mobility is currently the top area of concern for IT professionals around the world. The rise of employees (frequently senior employees) bringing in their own device (BYOD – bring your own device), accessing the company network and using company information has meant that IT is losing the battle for control.

Figure 3: What challenges are creating the biggest security headaches for your organisation?[5]



Rather than trying to prevent BYOD, the focus now is to find a way of managing it. Not a small task – given there are so many device types, operating systems, mobile applications and the 'invisibility' that comes from employees simply plugging in (wired or wirelessly) and accessing what they need. Yet more complexity, yet more to manage.

This combination of IT change coupled with changing work patterns and business demands creates real tension in balancing resource, cost and security.

4 Worldwide Smartphone Market Expected to Grow 55% in 2011 and Approach Shipments of One Billion in 2015, According to IDC, 09 June 2011, http://www.idc.com/getdoc.jsp?containerId=prUS22871611
5 Source: Bathwick Group, 'Security readiness in a changing technology landscape', March 2012

The threat landscape: a new era of sophistication

3.0

- More than 67 million unique threats on Kaspersky's database[6]
- Threats increase by 125,000 per day[6]
- 140 new mobile malware threats every day[6]
- 91% of organisations have experienced at least one threat in the last 12 months[7]

Two words sum up how cyber security risks have evolved in the last few years: volume and sophistication. As proof, Kaspersky's Global IT Risk Survey of 2012 found that 91% of organisations have experienced at least one attack in the preceding 12 months.

The level of sophistication seen in malware has escalated to the point where many believe that 'traditional' anti-malware is no longer enough. At the extreme end of the malware landscape, Stuxnet and Flame have grabbed headlines for not only the damage they have caused, for going undetected for so long. Flame, for example, has been in existence for years and was only formally identified in May 2012.

3.1 A new breed of threat sophistication

These examples point to the fact that there is now a higher 'entry level' for cyber criminals: viruses are more sophisticated and exploit vulnerabilities with the explicit intent of stealing valuable data.

Business bank accounts are a prime target since they carry high balances but often the account holder may not take adequate security measures. This certainly explains the increasing volume of Trojans, and malware such as Zeus that steal information and enable hackers to compromise corporate finances.

And this trend has been borne out by the rise of Advanced Persistent Threats (APTs). Governments and global corporations are not the only targets of highly-sophisticated malware attacks – small businesses are equally at risk. Moreover, as cyber criminals make more use of such threats, there's a greater risk of collateral damage – so even organisations that are not the intended target can end up in the firing line.

3.2 Moving up the infrastructure stack

This degree of sophistication and determination brings the average organisation's IT security requirements into a whole new paradigm. The starting-point for many of today's attacks is exploiting vulnerabilities in commonly-used applications. In the past, Windows itself was the main focus of activity for those looking for vulnerabilities that could be used to install malicious code on a computer. But the regular release of security updates from Microsoft in recent years has led cybercriminals to shift their focus to non-Windows applications. So much so that Windows doesn't even figure in the top 10 vulnerable software packages (see Figures 4 and 5). Unfortunately, many applications remain unpatched for long periods of time.

6 Source: Kaspersky Lab
7 Source: Kaspersky 2012 Global IT Risk Survey

According to securelist.com, more than 80 per cent of all vulnerabilities target Java and Adobe Acrobat Reader[8]. Not only is Java installed on many computers (1.1 billion according to Oracle), but updates are installed on-demand – not automatically. In the case of Adobe Acrobat Reader, it's only recent versions that include automatic updates. Users are accustomed to downloading applications to their PCs and smartphones, creating dozens of managed and unmanaged applications, each carrying a number of potential vulnerabilities.

The increasing diversity of device and operating platforms on which businesses transact data only amplifies the security challenge: quite simply, there is more to manage, and more gaps to fill.

The volume of security vulnerabilities have shifted to these platforms, but the increasing number of operating systems and the tens of thousands of applications written for them are making it nearly impossible to chronicle and remediate vulnerabilities. This trend is seen in the diversity of vulnerable applications and operating systems (see Figures 4 & 5).

Figure 4: Most Targeted Applications[8]

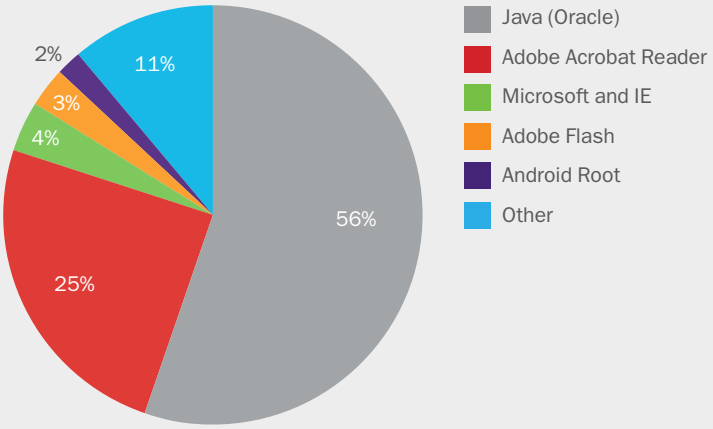


Figure 5: Top 10 Software Vulnerabilities, First Quarter, 2012[9]

Rank	Vulnerable Application	% of Vulnerable Users	Rating
1	Oracle Java (multiple vulnerabilities)	35%	Highly Critical
2	Oracle Java (three vulnerabilities)	21.7%	Extremely Critical
3	Adobe Flash Player (multiple vulnerabilities)	19%	Highly Critical
4	Adobe Flash Player (multiple vulnerabilities)	18.8%	Highly Critical
5	Adobe Reader/Acrobat (multiple vulnerabilities)	14.7%	Extremely Critical
6	Apple Quick Time (multiple vulnerabilities)	13.8%	Highly Critical
7	Apple iTunes (multiple vulnerabilities)	11.7%	Highly Critical
8	Winamp AVI/IT File Processing	10.9%	Highly Critical
9	Adobe Shockwave Player (multiple vulnerabilities)	10.8%	Highly Critical
10	Adobe Flash Player (multiple vulnerabilities)	9.7%	Extremely Critical

8 Source: https://www.securelist.com/en/analysis/204792250/IT_Threat_Evolution_Q3_2012#4
9 Source: https://www.securelist.com/en/analysis/204792250/IT_Threat_Evolution_Q3_2012#14

The threat landscape: a new era of sophistication

Protecting leaks:
the rise of data encryption

- 15% of organisations have experienced data loss as a result of theft of mobile devices [11]
- Malware and spam are still the biggest causes of data loss [11]
- Data encryption is ranked as no.2 on the list of areas most organisations would like to improve.[11]

3.3 The mobile dimension

Mobility adds a new dimension to risk. Today, Apple's iOS, OS X and Google's various flavours of Android operating systems are as prolific as Windows.

Cyber criminals are well ahead in exploiting the risks that mobility brings. In Q2 2012, the number of Trojans targeting the Android platform nearly tripled from Q1 2012 (See Figure 6).

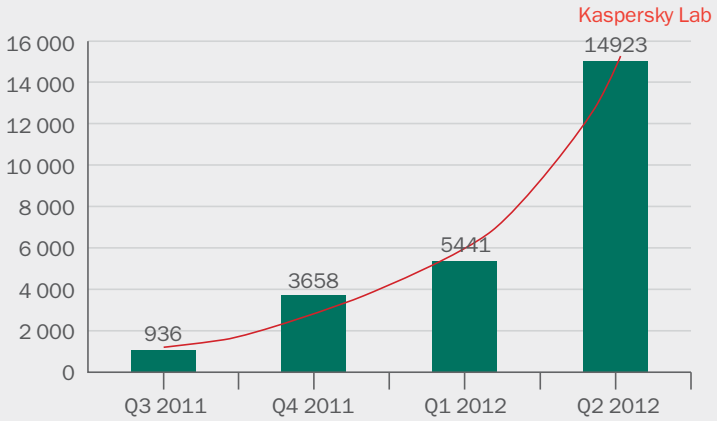


Figure 6: The number of malware modifications targeting Android OS[10]

This is set to increase, as the ease of which a business person's mobile data can be taken or intercepted makes mobility a new battleground for cybercrime.

Kaspersky's 2012 Global IT Risk Survey highlighted the trend of 'bring your own device' (BYOD) and shows more and more organisations are allowing the owners of these devices to access corporate data and networks, without any additional security measures. This surprisingly liberal approach comes down to a number of factors, but principally the rate of uptake of devices, and the fact that there are simply too many different device types and OS versions for an under-resourced IT team to manage.

Wireless connectivity, cloud services and file-synchronisation applications are making these devices highly desirable targets for physical theft.

Thieves and hackers with access to stolen mobile devices will compromise them to steal valuable data or use them to penetrate corporate networks. The direct monetary damage of device loss and theft is estimated at $7 million annually[12]; the indirect costs of any associated hackings are unknown.

3.4 Social business – restrictions are dropping as the risks start to grow

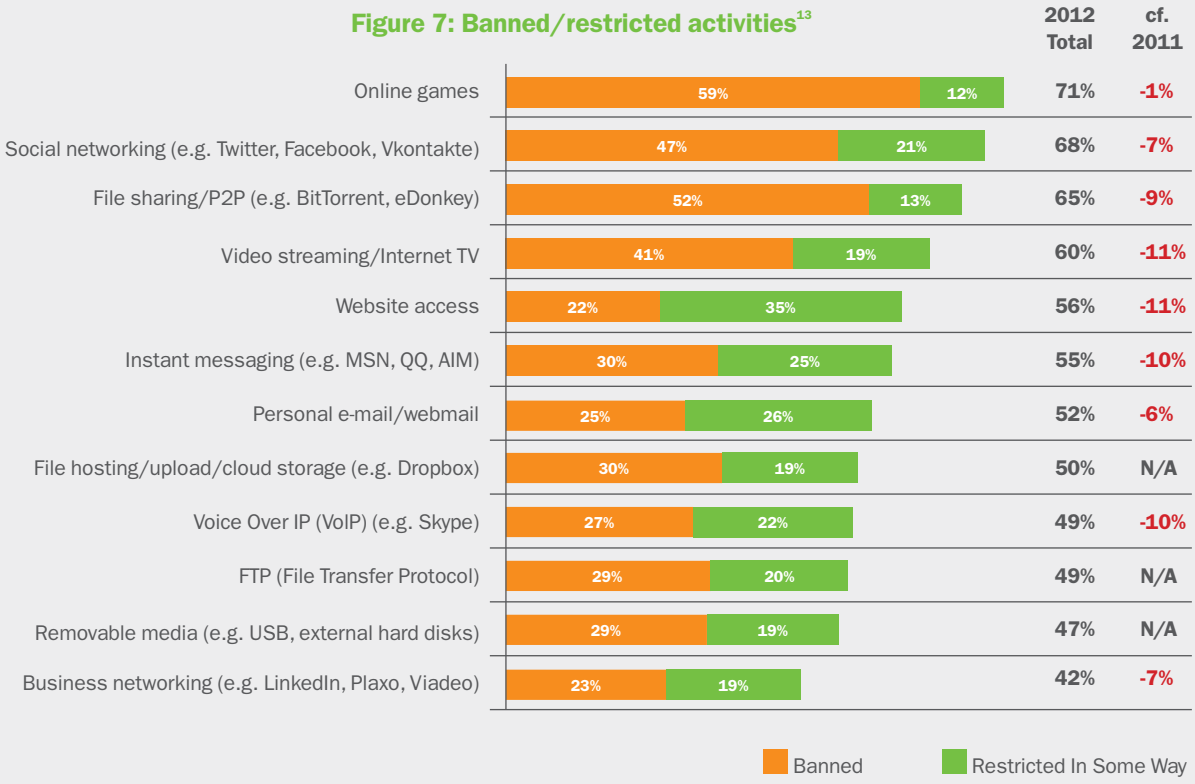
IT administrators rightly point out that the biggest security risks are not down to technology itself, but people. Ubiquitous social media and web usage – and people's desire to be 'always-on' – are making it harder and harder for IT teams to manage security risks.

10 Source: securelist.com Q2 2012 report: http://www.securelist.com/en/analysis/204792239/IT_Threat_Evolution_Q2_2012
11 Source: Kaspersky Global IT Risk Report 2012
12 Source: https://www.lookout.com/resources/reports/mobile-lost-and-found/billion-dollar-phone-bill

The hottest topic is social business. It is seen as one of the highest threats to IT security, and remains the second most closely controlled, with just over half of organisations banning it outright (see Figure 7). Restrictions around social media and web usage are dropping, though it's hard to determine whether this is down to IT 'losing the war' or because the business benefits of social and web usage are too great.

David Emm, Senior Regional Researcher at Kaspersky, commented *"To outlaw the 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."*[14]

Figure 7: Banned/restricted activities[13]



The alarming conclusion though, is that organisations have not worked this part out. Managing the use of social media and guarding against unfettered web usage will be a major facet of the well protected organisation in the future. This is less due to 'inherent risks' of social media, more due to the users clicking on adware and surveys embedded in social media, and even more due to the general 'sharing' attitude which seems to have arisen. FTP sites, file hosting and uploads open up many serious IT security risks but are seen by many as legitimate and safe.

IT teams need to realise the extent and severity of these new dangers, and their prevalence within their end-user community. Only then will organisations of all sizes make an objective reassessment of their current security posture and approach.

13 Source: Kaspersky 2012 Global IT Risk Survey
14 Source: Kaspersky Global IT Risk Report 2012

Simplifying the picture: a single platform

4.0

Many angles, many solutions: protecting the business is a complex matter

- 44% now protect sensitive data via encryption
- 33% allow 'uncontrolled' network access via smartphones[15]

4.1 Why the IT security industry has only made it harder

The IT security industry has, so far, not made it easier for organisations. The proliferation of different technologies has, until now, been responded to by 'point solutions'. In itself this is not unusual, and just a symptom of a maturing market and evolving technologies.

In organisations where there is not a dedicated IT security team, the multi-tasking IT departments have a bewildering and frustrating experience dealing with what's on offer from the industry. Finding, evaluating and buying what they need is complex task in its own right.

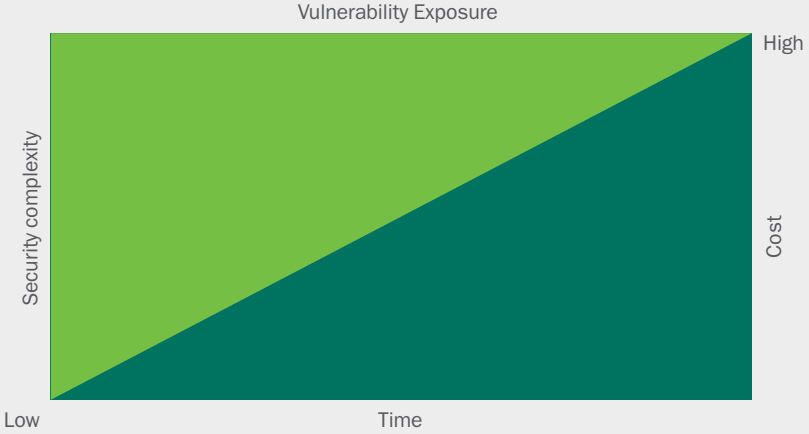
Organisations will frequently be using conventional anti-malware for their core endpoint security. They may have added encryption to email and file sharing systems. If they have a mobile end-user population they may have invested in mobile device management (MDM) technology to control and contain the influx of both company-sponsored and BYOD devices. And on top of this, they will have some kind of approach to patch management – to track and push software fixes across their operating environments to prevent applications from becoming security breaches.

So investments may well have been made, but a much bigger challenge will have arisen.

Security systems simply don't talk to each other. Every time a systems administrator runs a report, implements a change, responds to an alert or updates software, they must go to a different management console for each specific application. This manual co-ordination of supposedly 'connected' technologies is inefficient and highly time-consuming (see figure 8). Above all, it is the enemy of security effectiveness.

For instance, if you have five different security applications, and it takes five minutes to perform a single function on each platform to engage in a coordinated security action, it will take 25 minutes overall to implement the change. Add the effort required to verify that the change was implemented properly, as the reporting mechanisms for each application are different. The net result is a security administrator who will spend hours sifting through reports and screens to perform a function that should be relatively automatic.

Figure 8: Complexity is the enemy of security efficiency and effectiveness. The higher the complexity of security technologies and the more time it takes to effect change, the greater the security cost and the lower the return on security investment.[16]



15 Source: Kaspersky 2012 Global IT Risk Survey
16 Source: 2112 Group – Complexity is the enemy of security. October 2012.

"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 and Services[17]

Whilst 'integration' is a much over-used term in the IT industry, it is critical to improve security posture. It is impossible for resource-limited teams to manage multiple systems, oversee multiple dashboards and then take corrective action.

The speed of identification and response is particularly important in IT security – in a normal network environment the longer applications stay unpatched, the bigger the window of vulnerability. Then take this scenario and extend it across today's complex environment comprising mobile devices, virtual machines and employee-owned devices. Implementing changes quickly and easily is a critical component of taking an effective approach.

The reason why 'integration' is such a problematic term in this context is that many 'consolidated' approaches have been created simply by stringing together different point solutions. In itself this isn't a problem, the technologies will certainly 'work' together – but it's not a seamless process. And most importantly, it's not a fast one: it takes manual effort to understand the different interfaces, ensure policies are consistently and correctly applied across different 'joined together' technologies.

Time is a challenge and it is something that already stretched IT teams don't have. What's needed is a singular way to perform multiple tasks in all sorts of different environments.

17 Source: Kaspersky Global IT Risk Report 2012

You can’t protect what you can’t see: simplified management brings new visibility

5.0

5.1 The cost and resource conundrum
As businesses adopt more and diverse technologies, embrace mobility and collaboration, and become reliant on data-driven operations for continuity and productivity, it is paramount to improve the security posture and reduce risk and exposure to hackers and malware. Unfortunately, this inevitably means security needs are not commensurate with resources; increased IT spending doesn’t mean extra staffing and expertise.

IT security vendors are looking to create and market applications and tools that feature greater interoperability and integration. Today, large enterprises accomplish this through customised systems that aggregate and standardise reporting. But, this approach comes with extensive cost, and commitment to specialist in-house resource to support these systems – this is rarely an option for the majority of smaller businesses.

5.2 Breaking the mould – see, control and protect all your endpoints; all from one place
The future approach must start with a single platform, the often termed ‘single pane of glass’ that gives IT administrators a single view, and visibility they need to make an informed start on protecting their business and its data.

Visibility leads to control, and control leads to protection.

So for all but the larger enterprises, the solutions must avoid extensive management resource, not require systems integration and be administered by non-IT security specialists. This solution must still deliver a seamless way to see, control and protect whatever endpoints are carrying company data, whether they’re on basic desktops, virtual machines, tablets, smartphones or even employees’ own devices.

At the heart of this must lie a single, consistent management console. The security tools can then be accessed and controlled from a single dashboard with a consistent way of configuring, delivering and managing policies and security settings across
the organisation.

Conclusion

6.0

Kaspersky Endpoint Security for Business provides:

- Anti-malware
- Data encryption
- Mobile security and mobile device management
- Application, device and web control
- Systems management, including patch management

Kaspersky has recognised that for most organisations, securing and managing all the computing devices in the organisation has become a much bigger and more frustrating job. It is clear that tackling complexity can only be achieved by a singular, consolidated IT security approach. The needs and the issues discussed in this paper have led Kaspersky to develop a new approach – Kaspersky Endpoint Security for Business.

Kaspersky Endpoint Security for Business is fundamentally different to everything else on the market today – in that's it has been 'built from the ground up'. In other words, a single IT security platform rather than multiple pieces of software that have been linked together.

As a result, it makes maintaining your overall security posture far easier, as policies can be set once and then rolled out at the click of a button to multiple endpoint types, and environments.

Kaspersky Endpoint Security for Business provides a complete, fully integrated platform that gives you the world's best anti-malware protection, robust application control tools, plus system management, data encryption, and Mobile Device Management (MDM) —all managed from a single console. Protecting your data, managing your applications, and giving you the ability to see, control and secure all devices; whether physical, virtual or mobile; corporate or personal.

This means that at last organisations can achieve high levels of protection across a complex and frequently changing IT environment – but with minimum requirements for training and specialist knowledge. What were once considered complex, expensive and difficult-to-manage technologies are now a reality for all organisations, regardless of size or resources.

See it, control it, protect it. Now you can with Kaspersky Endpoint Security for Business

About Kaspersky

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 15-year history Kaspersky Lab has remained an innovator in IT security and provides effective digital security solutions for consumers, SMBs and Enterprises. The company currently operates in almost 200 countries and territories across the globe, providing protection for more than 300 million users worldwide.

Learn more at www.kaspersky.com/business