Ready... Or not?

Balancing future opportunities with future risks.

A global survey into attitudes and opinions on IT security.

Be Ready for What's Next.

kaspersky.co.uk/beready

KASPERSKY lab

Contents

Introduction and Executive summary

0.1

As the technology landscape evolves, businesses and their IT teams are facing an increasing threat to their security from a variety of cyber threats. This is felt in organisations across the world – nearly half feel cyber threats will be a top priority in the next two years and yet 45% don't feel fully prepared.

Survey highlights:

- 91% have been affected by attacks in the last year
- 45% are under-prepared for dedicated cyber attacks
- 17% have lost financial information as a result of attacks
- 57% have banned access to social networks due to potential security risks
- 30% have still not fully implemented anti-malware software

To get to the crux of these issues and give a clear view on the effects felt by organisations across the world today, we commissioned a comprehensive survey of 1,300 senior professionals, from small business to enterprise level, across 11 countries. The survey, produced by B2B International, was both in developed markets including the UK, USA and Japan and also developing markets including Brazil, China and India.

Those surveyed had an influence on IT security policy, a good working knowledge of IT security issues and knowledge of the wider organisation they worked in.

The findings were clear: cyber security is climbing the policy agenda in organisations across the board due to a perceived increase in viruses and data breaches. What's more, the devices and the people affected are becoming harder to both control and protect as they become increasingly mobile and opt to use their own technology as opposed to that supplied by the IT function.

Are businesses really ready for what's next?

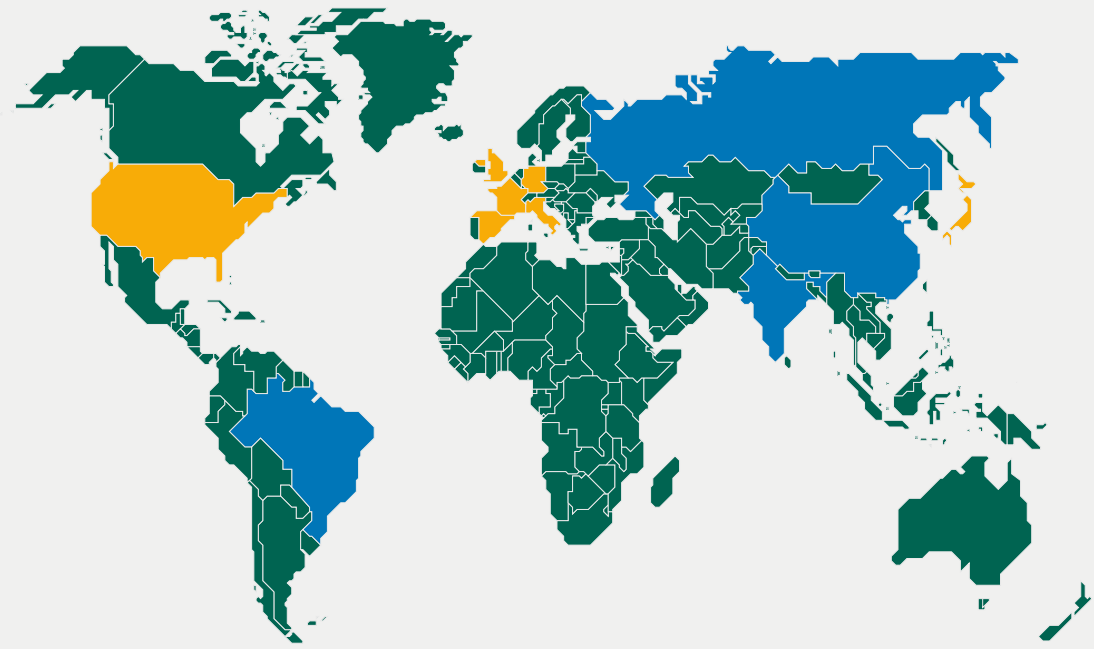
Countries covered

Developed Markets: (n=800)

USA	200
Germany	100
UK	100
France	100
Spain	100
Italy	100
Japan	100

Developing Markets: (n=500)

Brazil	100
India	100
China	200
Russia	100



IT security and the perceived risk to the business

1.0

JUST 14% REGARD CYBER THREATS IN THEIR TOP 3 RISKS

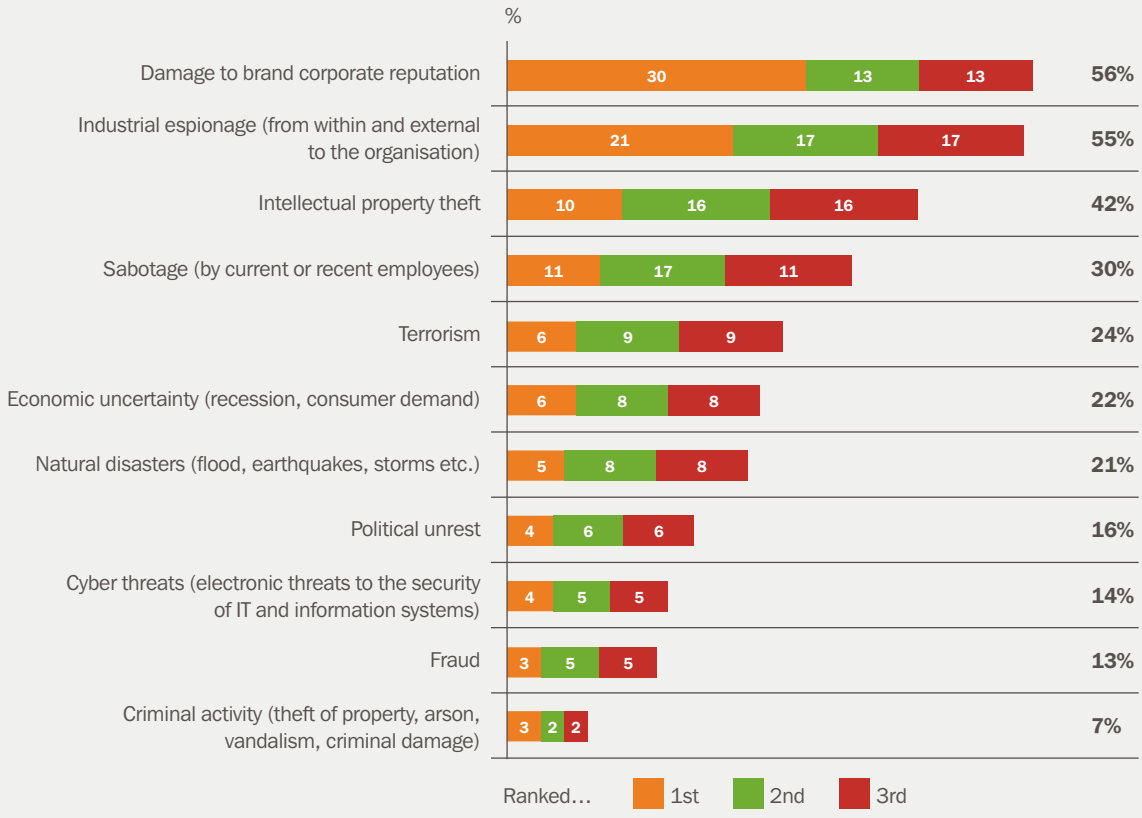
The fact is, businesses and the technology they use, are changing. IT network security is currently one of the top strategic considerations for organisations. Today, executives must consider and plan for the upcoming threats they may encounter. Just 14%, however, consider cyber threats specifically to be one of the top three risks to the organisation. This suggests a low general level of security awareness in businesses.

Interestingly, brand damage, industrial espionage and intellectual property theft were among the top businesses threats – all events that could be precipitated by an IT security breach. Conversely, however, the potential brand damage may be one of the main reasons attacks go unreported.

The danger for organisations across the globe is that in the majority of cases they may not realise they have suffered an attack or are an interesting target for criminals. IT teams need to consider that these threats are not just a possibility; moving forward the question is not 'if' you are breached, but 'when?' and how badly.

"9% of organisations have suffered from a targeted attack; I believe the number is probably higher, but many are not aware yet"
Costin Raiu

IT security and the perceived risk to the business:



The risk of devices out of your control

2.0

THREE QUARTERS OF ALL BUSINESSES GLOBALLY EXPECT AN INCREASE IN DEVICES OVER THE NEXT 12 MONTHS

IN SMALL ORGANISATIONS, THERE COULD BE 50 DEVICES CONNECTED TO THE INTERNET, AT ENTERPRISE LEVEL THERE ARE THOUSANDS

"The end-point is no longer just a PC, it can be any device – as long as it's smart enough and well connected"
Stefan Tanase

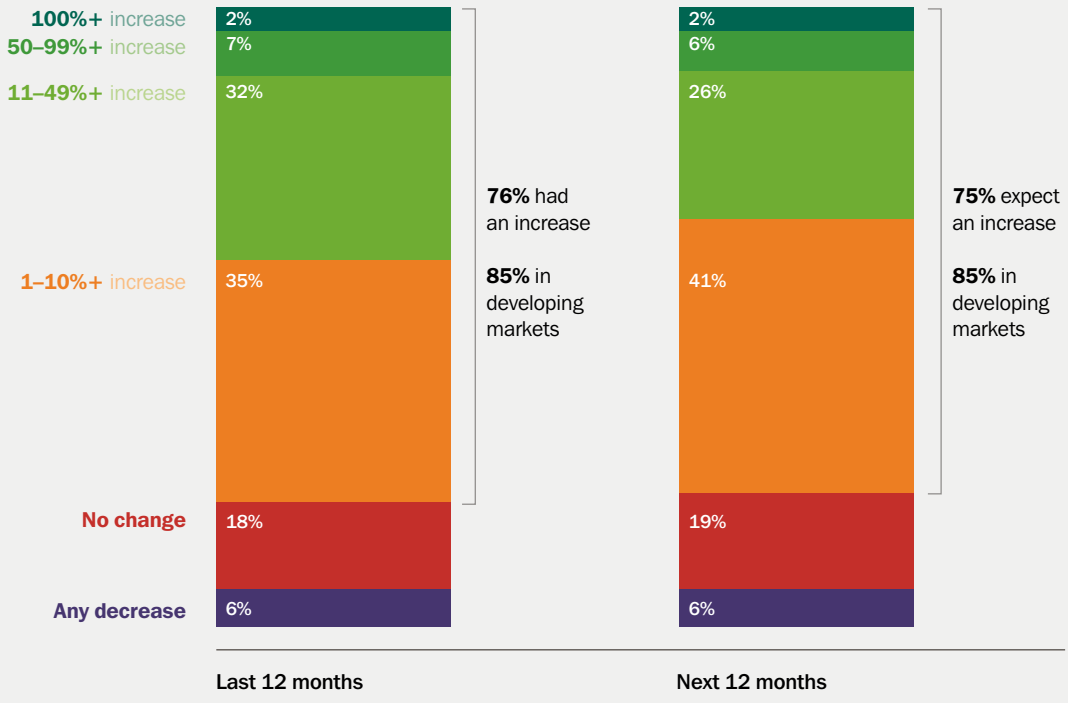
Until recently, each member of your workforce had a computer at their desk and a landline phone next to it. Although cyber threats existed, the endpoint devices were universal and easy to control.

Today the picture is different: the cost of smartphones and broadband internet connections continues to fall and the definition of an endpoint device is changing – from a PC, to any device that is 'smart' enough and connected to a network.

In a small business, there could be 50 or more of these devices connected to the internet, at Enterprise level there are thousands. More worryingly for IT teams, three quarters of businesses globally expect an increase in these numbers over the next 12 months.

For organisations across the world, a growing number of devices used by a workforce on the move means a growing number of threats. Not only are these devices, such as the iPad, harder for IT teams to control than PCs, but many of these devices often have no security software installed – meaning they are the new focus for cyber criminals.

Change in end user devices



The attack of the cyber criminals and ill-prepared systems

3.0

ALMOST HALF OF ALL ORGANISATIONS SEE CYBER THREATS AS ONE OF THE TOP 3 DEVELOPING RISKS

45% OF BUSINESSES ARE NOT 'WELL-PREPARED' FOR CYBER ATTACKS

"Almost half of businesses say they're under-prepared for cyber-attacks. Is this a sense of realism, or a sign they're not getting the necessary budget?"
Roel Schouwenberg

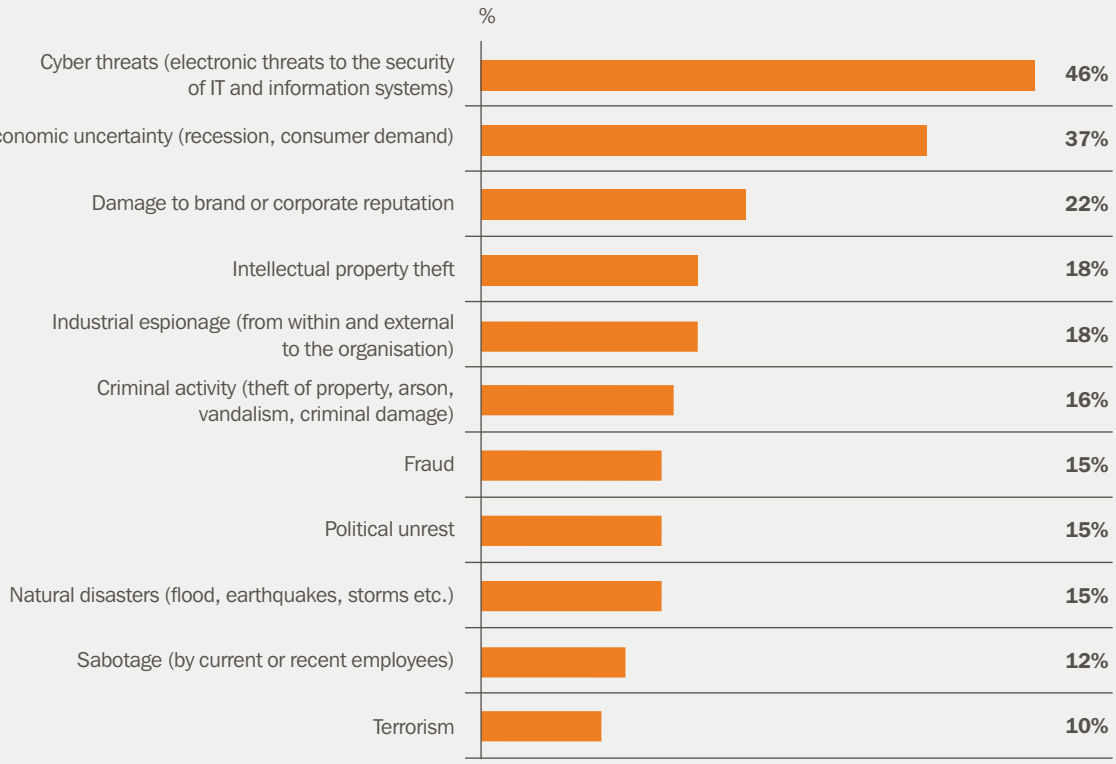
While businesses begin to become aware of threats from potential security breaches in the future, cyber criminals are on the attack today – targeting businesses that are under-prepared to deal with the threats they pose and will continue to pose in the future.

Just under half of organisations believe cyber threats will be much more important in two years' time, and understanding how to prevent IT security breaches should be the number one concern for the IT function across all regions. Despite this, only half of businesses feel well-equipped to deal with the impending issues, and among these the definition of 'well-prepared' may differ from organisation to organisation – leaving some more exposed than others.

This problem is magnified in small businesses. 45% don't see themselves as well-prepared for cyber attacks – implementing far fewer measures than larger businesses, such as a patch schedule to adequately serve their assets. This is often due to a lack of dedicated IT resource, whereas many large organisations may be able to afford a 24/7 IT team. The lack of preparation in all sizes of businesses also comes from budget cuts – if they are not at the top of the business agenda, the money is just not there to fully tackle the problem.

Increasing risks in two years' time

Almost half of all organisations see cyber threats as one of the top 3 developing risks



% Identifying risk as being much more important in 2 years

Organisations under threat

4.0

48% OF COMPANIES SAY THEY HAVE FELT AN INCREASE IN THE NUMBER OF CYBER-ATTACKS IN THE LAST YEAR

40% OF ORGANISATIONS HAVE SHOWN A CONCERN ABOUT GOVERNMENT INTERFERENCE WITH THEIR INFORMATION SYSTEMS

Despite a lack of preparation from IT teams and the wider business against the impending threats they face, organisations are feeling the heat. 48% of companies say they have felt an increase in the number of cyber-attacks in the last year, and over half are worried about involvement of organised criminal gangs in these. Possibly more important, 30% of organisations felt that they were being specifically attacked, however, these figures may be lower than anticipated as attacks often go unnoticed until a theft takes place.

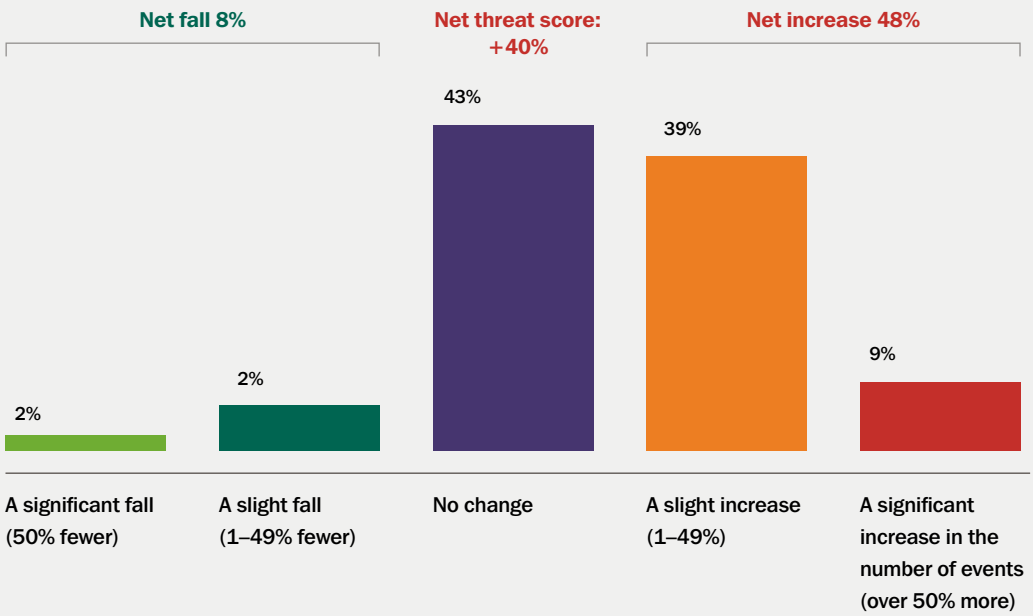
But it is not just cyber gangs that are on the radar for IT security teams. 40% of organisations have shown a concern about government interference with their information systems. This will mean that cryptography will ultimately need to become ubiquitous, and solutions that already exist – including whole disk encryption and virtual private networks – will need to be implemented to ensure higher levels of security.

Despite the majority of threats (61%) coming from malware and network intrusions, the threat for businesses is not just from external sources. Internally, the top vulnerability came from flaws in existing software – with 44% of organisations having a related incident in the last 12 months. Staff also pose an internal threat to data loss – 10% of organisations have been victims of fraud or sabotage from their own staff and 16% of organisations highlight intentional data leaks as their most concerning data threat for the future.

> "Generally, few people notice targeted attacks in the beginning and before the theft takes place"
> Costin Raiu

Perceptions of number of cyber threats

48% perceive an increase in the number of threats over the last 12 months



The impending dangers of new media

5.0

53% OF ORGANISATIONS HAVE BANNED SOCIAL NETWORKING SITES FOR END USERS TO SOME EXTENT

"File sharing peer-to-peer networks remains the main reason for worry in corporate environments and should be banned in every organisation that cares about security"
Costin Raiu

The threats from staff do not always come from intentional malicious attacks by the workforce. The online tools your employees use both in the workplace and at home can have a direct effect on your security. Viruses and malware spread through social networks and file sharing sites in particular can often cause problems for IT teams, no matter what the size of the organisation. Social networking, for example, is now seen to be the second biggest threat to IT security – with 57% of organisations viewing use of social media by employees as a significant risk to the business.

Those in control have responded to this by putting the lock on these networks. Over half of organisations have now banned social networking sites, and a further 19% restrict access in some way, making social networks the second most restricted activity within organisations across the world. We have, however, noticed that this does not work in reality as staff will always find a way to access these networks – whether at home or on their personal devices. Ultimately, educating the workforce in the security risks of using these networks is key to defending against this threat in the future.

Peer-to-Peer file sharing is still at the top of the security team's block list. 55% of organisations still see file sharing as the activity that is the greatest threat to their security – an activity that should be banned on networks and devices in any organisation that cares about security.

Organisations identifying an application/activity as one of the greatest threats

Activity/Application	Overall	Developing	Developed	United States	Russia	China	Brazil
File sharing/P2P	55%	46%	61%	62%	50%	44%	50%
Social networking	35%	36%	35%	44%	52%	26%	41%
File upload, File transfer, FTP	34%	33%	34%	33%	44%	28%	38%
Website access	32%	30%	33%	35%	42%	29%	19%
Personal email/webmail	31%	29%	32%	36%	22%	28%	32%
Instant messaging	23%	32%	18%	20%	19%	36%	35%
Online games	21%	21%	21%	19%	16%	21%	32%
Video streaming/internet TV	13%	18%	10%	8%	12%	21%	14%
Business networking	11%	15%	9%	5%	4%	24%	7%
Voice over IP (VoIP)	10%	14%	8%	5%	9%	17%	9%

Shaded cells denote countries/groupings where perceived threat is significantly higher

The reality of the damage to business

6.0

91% OF ORGANISATIONS HAVE EXPERIENCED AT LEAST ONE ATTACK IN THE LAST 12 MONTHS

16% OF ORGANISATIONS HAVE EXPERIENCED HARDWARE THEFT FROM THEIR PREMISES

Unfortunately for organisations across the globe, these are not just threats coming round the corner in the future – but real issues that are affecting them across the business every day. In the last year, 91% of organisations have experienced at least one attack, most commonly in the form of malware, subsequently followed by Spam and Phishing attacks. Of these, 24% have had their network intruded in some way – with 7% losing sensitive business data as a result, at a significant cost to the business.

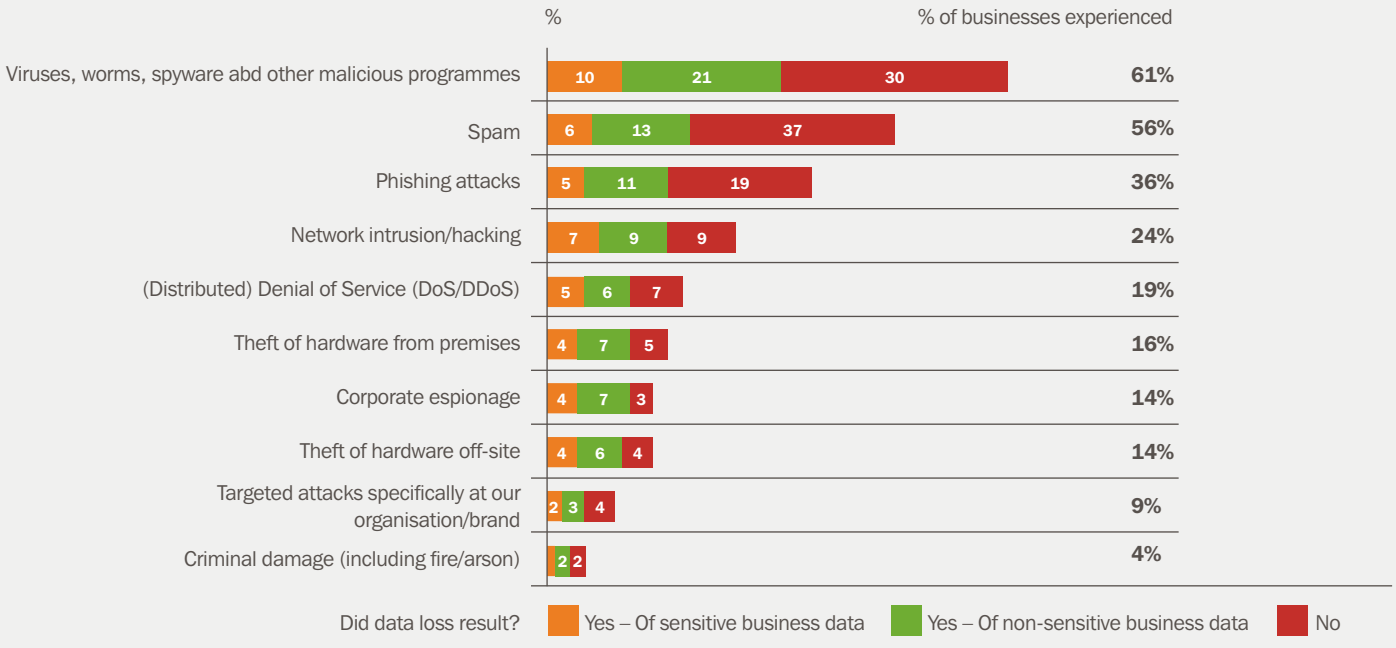
More of the attacks are also being specifically targeted. 9% of organisations questioned have suffered a targeted attack on their business in the last year – many losing some sort of intellectual property in the process. We feel this figure could in fact be higher, as many more organisations may have been specifically targeted but are not yet aware.

These threats also differ across markets. In developing countries, the levels of data loss are much higher, due to the lack of experience to correctly build and defend infrastructure against modern attackers.

It is clear that today the threats facing businesses are wide, coming in a number of shapes and forms. For example threats are not just web-based – 16% of organisations experienced hardware theft from their premises – one of the easiest ways to obtain credentials and information for later attacks. The result is that businesses must adopt an in-depth strategy, with multiple layers of defence, including anti-malware and full disk encryption to ensure a level of security as close to 100% as possible.

> "17% have lost financial information. This indicates that the main driver of cyber crime remains financial gain"
> Costin Raiu

The reality of the damage to business



How businesses are responding to the threats

7.0

30% OF ORGANISATIONS HAVE STILL NOT FULLY IMPLEMENTED ANTI-MALWARE SOFTWARE

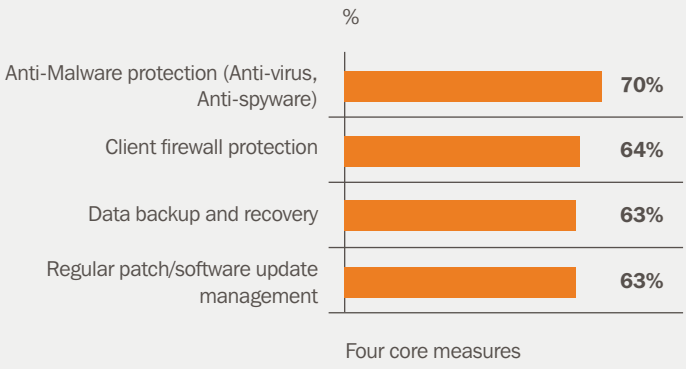
“It’s amazing that so many organisations don’t understand the need for such a basic security measure as anti-malware. While this is just one piece of a much larger puzzle, it should be considered part of the bare minimum necessities”
Tim Armstrong

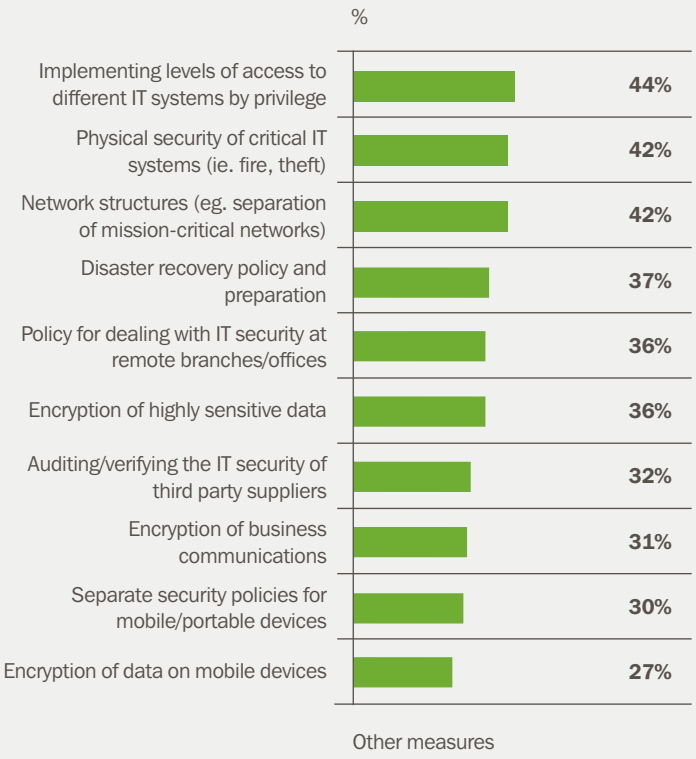
As these trends continue to develop, businesses globally are looking to the future as IT security and the impending threats continue to climb the agenda. For IT teams today, the most concerning external threat looking forward is network intrusion and hacking, whereas flaws in existing software is the top threat internally.

Sensibly, IT teams are starting to take measures to avert these security risks. Anti-malware protection tops the list of the ‘four core’ measures taken by organisations to protect their data – followed by client firewall protection, data back-up and recovery and regular patch and software update management. It is important to note that the top internal and external threats both come down to patching. Making sure all applications are patched will undoubtedly make it harder for an adversary to get inside your networks.

One of the most concerning findings is that a staggering 30% of organisations have still not fully implemented anti-malware software. With all the threats out there, as well as the potential implications for businesses who suffer an attack, it is shocking how many don’t understand the need for such basic security measures as anti-malware – something that should be considered the bare minimum of necessities.

Organisations have fully implemented different security measures





Are you ready for what's next?

7.1

Today, and in the future, cyber criminals will continue to pose a threat to businesses across the globe. It is clear that while many organisations are aware of the potential issues they face and are ready to protect their businesses, many are still not fully prepared.

You may have a workforce that is on the move – using a number of different devices that open you up to threats from cyber criminals. Whether you have been targeted in the last year, or are getting prepared for what is coming around the corner, it is essential for your organisation that IT systems and company devices are ready for what's next.

At Kaspersky Lab we ensure that you stay ahead of the threats to confidently take on new opportunities to help drive your business forward – and always Be Ready for What's Next.

For more white papers, videos and insight visit:
kaspersky.co.uk/beready

The Kaspersky Lab commentary team

Costin Raiu
Director of Global Research & Analysis
Kaspersky Lab

Stefan Tanase
Senior Security Researcher
Kaspersky Lab

Roel Schouwenberg
Senior Security Researcher
Kaspersky Lab

Tim Armstrong
Security Researcher
Kaspersky Lab