VansonBourne

Protecting the organization against the unknown

A new generation of threats

February 2014

Contents

Scope of the research

Research methodology

Dell commissioned independent technology market research specialist Vanson Bourne to undertake the research upon which this report is based. IT decision-makers from private sector organizations with 500 or more employees, and from public organizations with 500 or more end users, participated in this study.

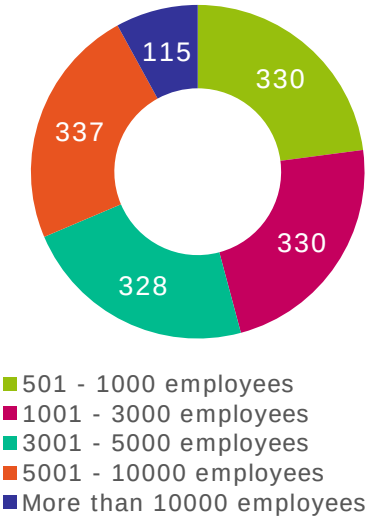

Figure 1: How many users (including employees, consultants, temporary employees, outsourced and remote employees, and partners) are there within your organization?" *(1440 respondents)*

A total of 1440 interviews were undertaken during October and November 2013. These were conducted using both online and telephone methodologies. Interviews were performed in a total of ten countries:

- US – 300 interviews
- Canada – 60 interviews
- UK – 200 interviews
- France – 200 interviews
- Germany – 200 interviews
- Italy – 60 interviews
- Spain – 60 interviews
- India – 200 interviews
- Australia – 60 interviews
- China (Beijing area only) – 100 interviews

Aims of the research

In recent years, security breaches (from loss of data to identity breaches) have led to millions of dollars of cost. With vast amounts of data at risk, organizations need to protect themselves as best as they can. Although many businesses already have solutions to protect against known threats, there is a new generation of threats that are unknown, against which organizations may not be protecting themselves at all. Unknown threats such as poorly configured systems, ineffective data governance, poor access management and inadequate usage policies could cause significant problems to enterprises.

Such threats come from both inside and outside the organization, prompting the need to reassess how organizations protect all their perimeters; this includes the organization's physical IT environment, virtual network, and accidental or intentional sabotage by employees. Failure to protect themselves could cause unwelcome disruption which is likely to hinder business performance.

There are a number of big trends which are acting as silent predators for businesses, such as vulnerabilities brought by BYOD, cloud, and internet usage. These unknown threats have the potential to be very costly for IT departments and organizations as a whole.

This research was commissioned to evaluate how organizations are preventing security breaches and whether IT security is a priority for them over the next twelve months as well as in the coming years. How have security breaches impacted an organization's approach and understanding of security threats? And how are organizations protecting themselves from potential vulnerabilities associated with the adoption of BYOD, cloud, and increased internet usage?

Summary of key findings

17% of the IT budget/revenue is allocated to IT security

- In the private sector this equates to an average annual spend of $96 million, and an average annual spend of $62 million in the public sector
- Respondent organizations that have not experienced a breach are allocating an average of 12% of their IT budget to IT security…
- …and those that have experienced a security breach are dedicating an average 18% of their budget to IT security. This indicates that those that suffer a breach are more likely to commit resources to avoid a repeat of the problem

In the next 2-3 years, 74% are planning to increase their spend on IT security

Almost nine in ten (86%) will be prioritizing security next year…

- …for 38%, security will be their top priority

Almost three-quarters (73%) are using cloud to host their data or apps…

- …but only 46% are currently using cloud security

73% have experienced a security breach in the last twelve months

83% have security processes that enable them to immediately identify a security breach…

- …however, actual detection of the most recent security breach took an average of seven hours

There is a lack confidence in current solutions

- 40% do not believe that their IT solutions fully equip them to prevent security breaches
- Respondents experience an average of three barriers that prevent better/more security measures being implemented

53% see the government's role in security as helping their organization's operational effectiveness

76% recognise that their security must protect them from both insider and outsider attacks

IT security in organizations

The current landscape

On average, those surveyed are currently spending a fifth of their annual revenue/budget on IT; 17% of this spend is being allocated to IT security. In monetary terms, this equates to private sector organizations spending an average of $96 million on IT security annually, and public sector organizations spending $62 million.

Spending on security has increased in the last 12 months, across a variety of different areas.

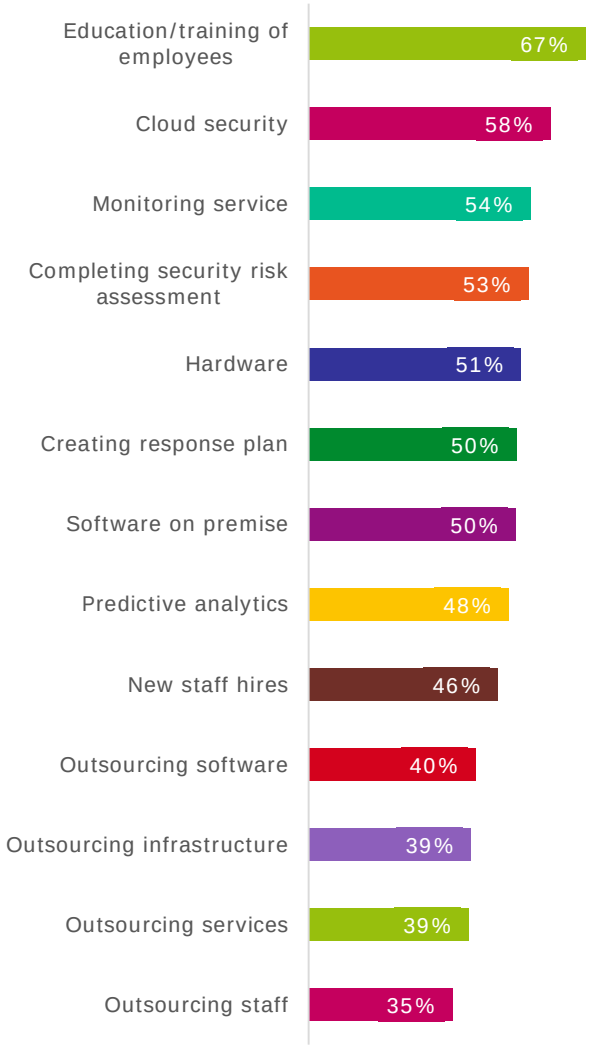

Figure 2: Those selecting spending has increased for "In the last 12 months, in which of the following areas within security have you increased/decreased spending?" *asked to all respondents (1440 respondents)*

Organizations are spending more on cloud security (58%) than on hardware (51%) or on on-premises software (50%), suggesting a move towards greater usage of cloud services.

On a monthly basis, around two in five (39%-45%) respondents often spend time on activities to combat/detect security breaches, ranging from responding to security threats, to educating their teams on new security measures or best practices.

However, organizations are being more reactive than proactive with their IT security resourcing. Those that have experienced a security breach are more likely to spend more time sharing information about potential vulnerabilities than organizations that have not. They are also more likely to be developing strategies to protect against vulnerabilities with cloud and BYOD. Organizations are therefore reacting to big IT trends, rather than spending money protecting the organization from unknown threats before suffering a breach.

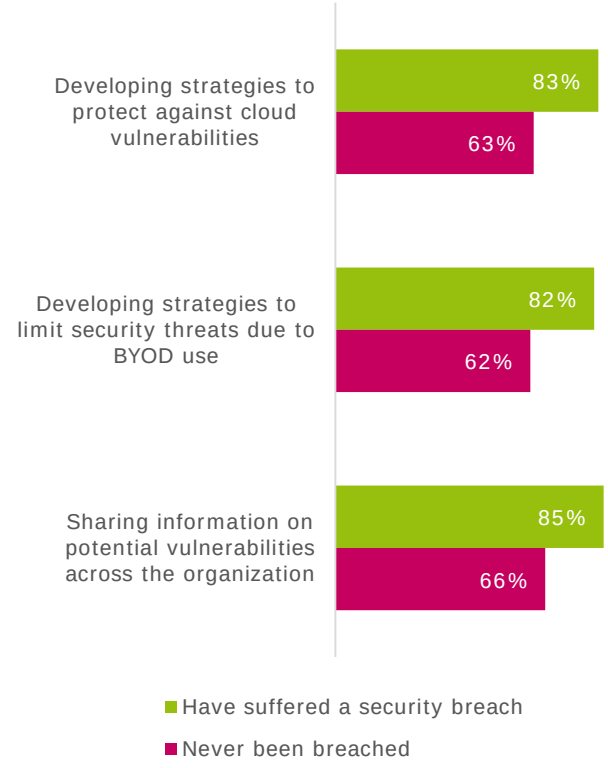

Figure 3: Those selecting sometimes or often for "On a monthly basis, how much time is spent on the following activities?" *analyzed by whether a breach has occurred (1440 respondents)*

Similarly, those that have experienced higher costs as a result of a security breach are spending more time developing strategies to protect against cloud vulnerabilities than those that have not suffered as much.

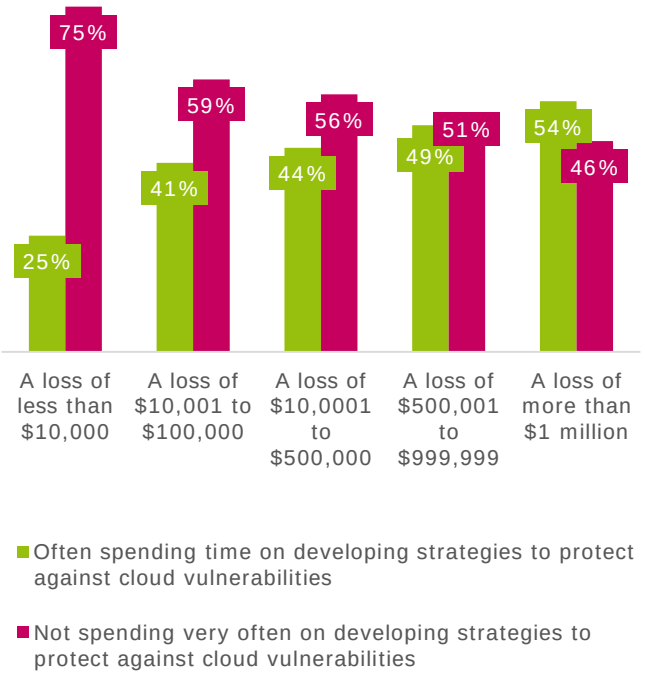

Figure 4: *Time spent on developing strategies to protect against cloud vulnerabilities, analyzed by how much have security breaches have cost the organization in the last twelve months (973 respondents)*

Future outlook

Security spending is set to increase for 68% of respondent organizations over the next year and 74% report that spending will increase over the next 2-3 years. Only a very small minority (3%) expect their spending on IT security to decrease.

91% of respondents whose organizations expect IT security to be their top priority next year indicate that their spending in this area will increase. This is significantly more than organizations where IT security will not be the top priority in the next twelve months (64%). If an organization prioritizes security, it will inevitably commit greater resources to it than those not prioritizing it. However, spending is still increasing for the majority of organizations; even if they are not prioritizing security next year, it is still important enough to them to allocate appropriate resource to it.

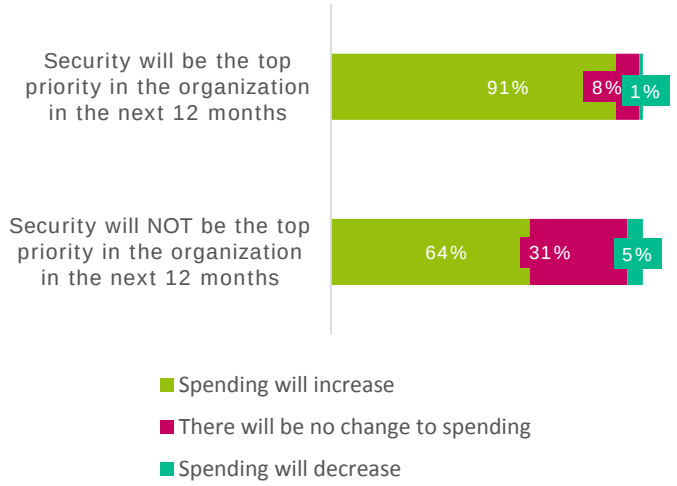

Figure 5: "In the next 2-3 years, how do you think your organization's spending on security will change?" *analyzed by if security is a priority for the organization in the next year (1440 respondents)*

Increased spending may be the result of the vast majority (98%) of respondents admitting that they are concerned about security. Losing critical business data is the top security concern for almost half of respondents (48%). This further explains why organizations are providing and are likely to continue to provide funds to implement security measures.

Those surveyed consider the increased usage of the internet, BYOD and cloud as their greatest threats over the next 5 years. These all potentially present vulnerabilities which may lead to an organization being penetrated by unknown threats. 49% of IT decision-makers surveyed are aware that these big trends have the potential to expose them to attacks.

Unknown threats are part of the next generation of risks. Yet only 18% of respondents list predicting and detecting unknown threats (such as advanced persistent threats or disgruntled employees) as one of their organization's top three concerns. This proves that unknown threats are yet to be prioritized by many.

Neither are these threats expected to be a significant concern in the near future, in the opinion of 37% of those surveyed. That said, respondents in larger organizations express more concern (50%) about unknown threats than those in smaller organizations (31%). Unless IT decision-makers prioritize understanding and combating unknown threats now and in the

future, they are likely to leave their organizations exposed to potential breaches.

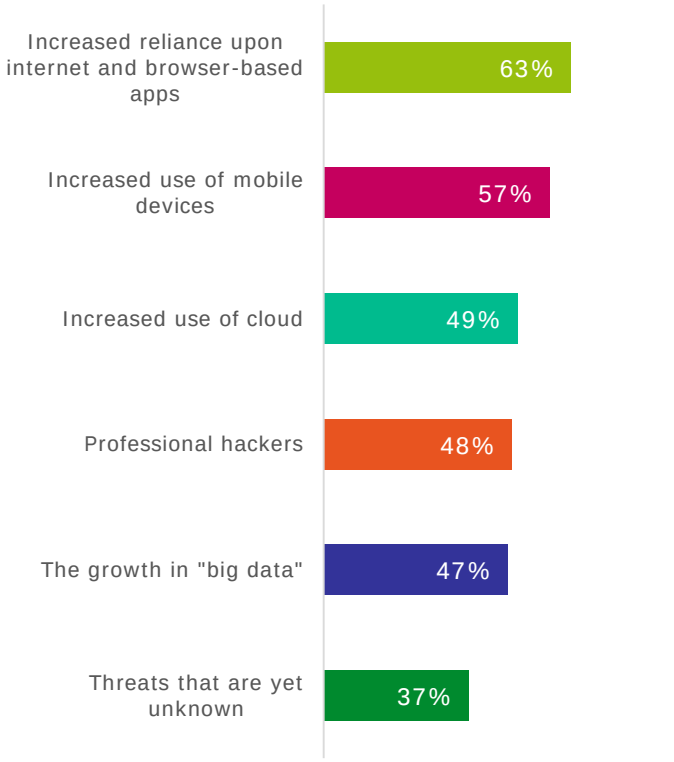

Figure 6: Respondents which ranked the answer first, second, or third for "Please rank the following options in order of greatest security threat to your organization in the next 5 years", *asked to all respondents (1440 respondents)*

Those surveyed consider the increased usage of the internet, BYOD and cloud as their greatest threats over the next 5 years. These all potentially present vulnerabilities which may lead to an organization being penetrated by unknown threats. 49% of IT decision-makers surveyed are aware that these big trends have the potential to expose them to attacks.

Country differences

US respondent companies in particular are investing more heavily in security than those in other regions. Respondents in this region say that on average their organizations have spent the most on outsourcing compared to other countries.

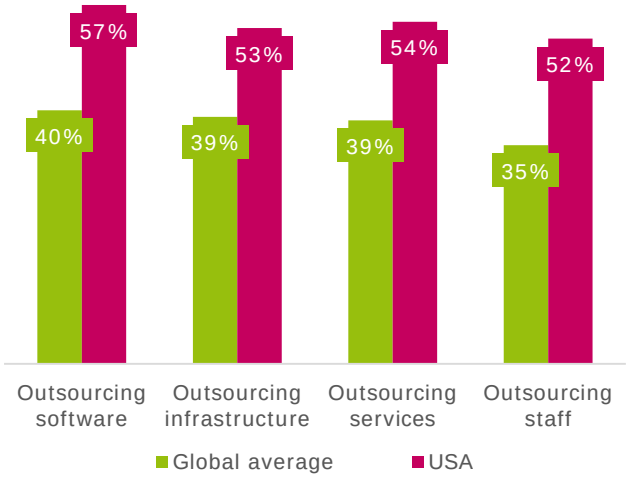

Figure 7: "In the last 12 months, in which of the following areas within security have you increased/decreased spending?" *analyzed by region*

The higher level of investment in outsourcing in the US compared to the global average correlates with a large proportion of organizations in this region adopting cloud.

Conversely, 17% of those surveyed in Spain are looking to decrease security spending next year, compared to the global average of 3%. This may be explained by the businesses looking to reduce all costs in times of economic hardship.

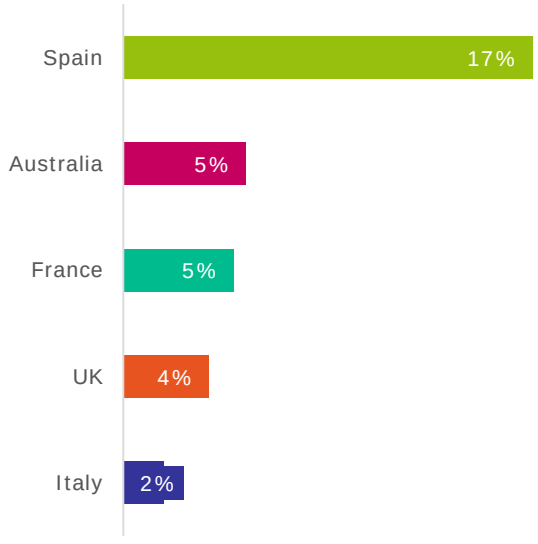

Figure 8: *Those that say that their security spending will decrease in the next 12 months, analyzed by regions which are higher than the global average*

Current policies and strategies

Inside the organization

Although over two-thirds are intending to increase their spend on IT security, all IT decision-makers surveyed are also aware of how the business is and will be, affected by internal and external policies and constraints. At present, many respondents consider the policies and strategies in figure 9 to be of high importance in preventing a security breach:

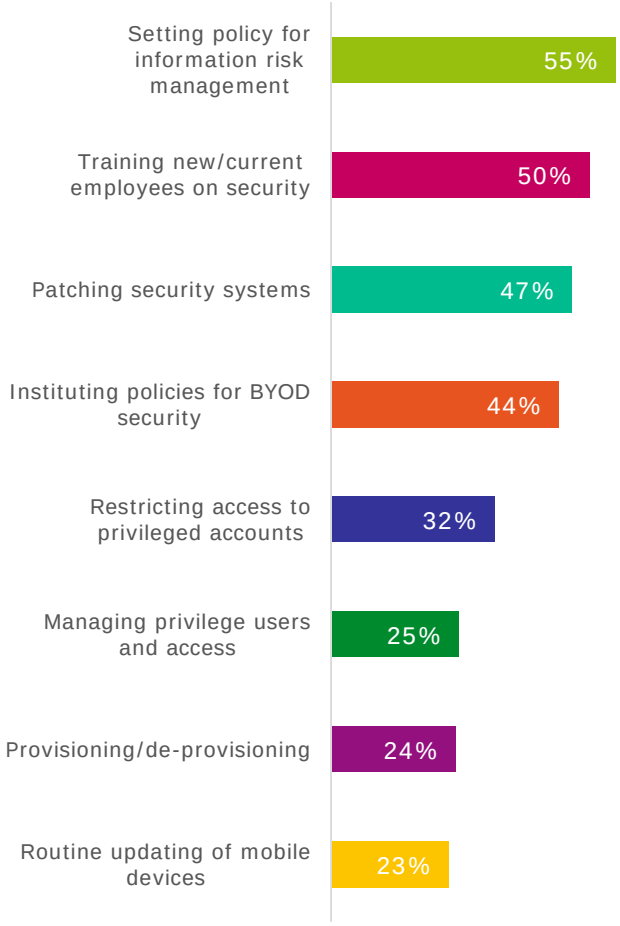

Figure 9: Those ranking each option first, second or third for: "Please rank the importance of the following policies and/or strategies in preventing security breaches?" *asked to all respondents (1440 respondents)*

Half or more of IT decision-makers surveyed are prioritizing the setting of policies for information risk management (55%) and training new/current employees on security (50%). However, few are prioritizing BYOD security: Less than a quarter (23%) routinely update their mobile devices and a little over four in ten (44%) are instituting policies for BYOD security as a matter of high importance. Failing to prioritize BYOD security could leave their organizations vulnerable to attack.

These policies and strategies are likely to be revisited over the next twelve months, as the vast majority (86%) of respondent organizations are prioritizing security over this time frame. 98% report that security will be a priority for their organization to some extent over the next year.

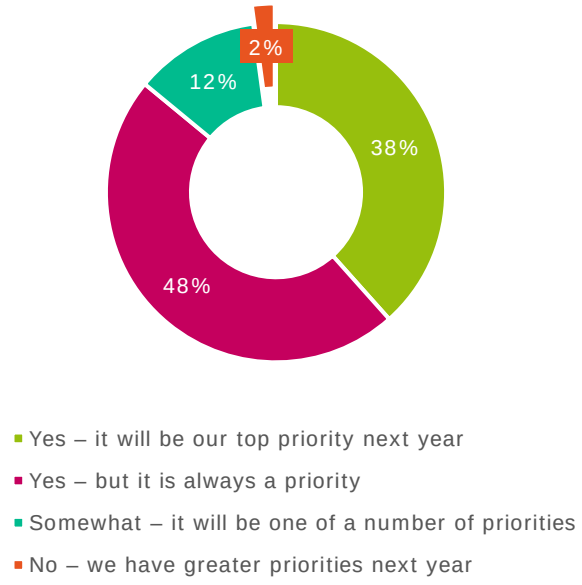

Figure 10: "Will security be a priority for your organization in the next 12 months?" *asked to all respondents (1440 respondents)*

Government influence upon the organizational policies

As a consequence of increased security threats, governments are playing a role in determining organizations' security strategy for the majority of those surveyed (84%).

Over half (53%) report that their government's role in security is helping operational effectiveness, with only 17% of IT decision-makers surveyed claiming that their government is hindering their organization's operational effectiveness for security.

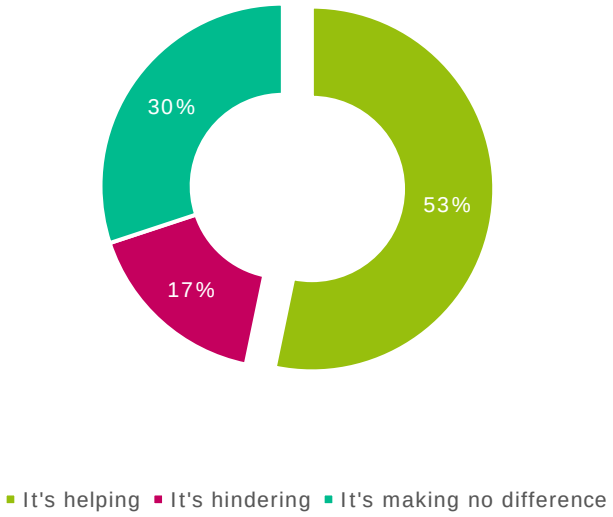

Figure 11: "How is the role the government plays in security affecting the operational effectiveness of your organization?" *asked to all respondents (1440 respondents)*

A lack of confidence in current solutions

Despite having internal strategies/policies and external assistance, four in ten (40%) do not believe that their current processes are fully equipped to protect them against future security challenges. Therefore, fewer than two-thirds (60%) have long-term strategies in place to equip them against future security risks.

IT decision-makers surveyed report an average of three barriers preventing them from implementing more or better security measures. There is no single barrier experienced by the majority, suggesting that different organizations will need customized guidance and support to suit their circumstances.

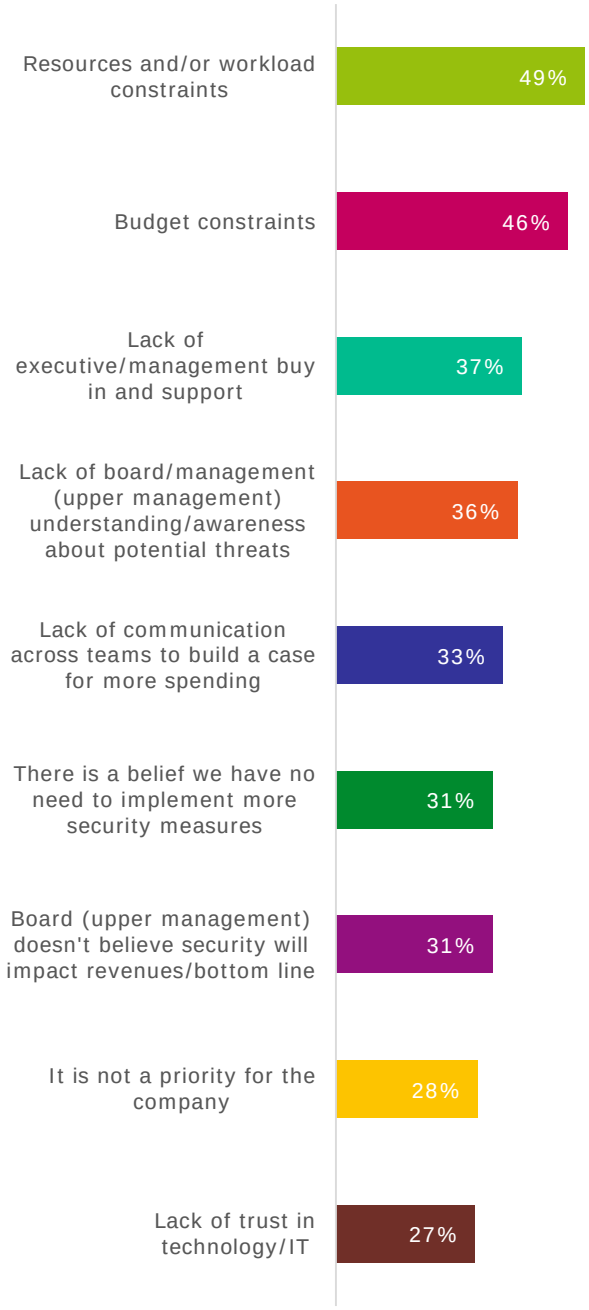

Figure 12: Those selecting each of the above as a big/major barrier for: "What are the main barriers that prevent your organization from implementing more/better security measures?", *only asked to respondents whose organization' security processes are not completely equipped to tackle future challenges (570 respondents)*

More than a quarter (27%) have a lack of trust in technology/IT, which may be holding them back from implementing better/more security measures in their organisations.

Country differences

Over 7 in 10 (71%) IT decision-makers surveyed from US companies claim that security will be their top priority in the next twelve months. This is compared to the global average of only 38%.

Those in the US are more likely than other regions to claim that their organizations have long term strategies in place to protect against security breaches.

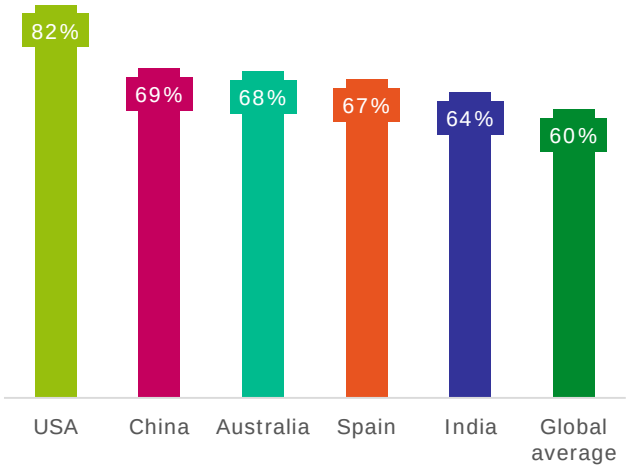

Figure 13: Those who say that they have long term strategies in place for "Do you think your organization's current security processes are equipped to tackle future challenges?" *analyzed by regions which are higher than the global average*

Responding to security threats

Most organizations are committed to preventing security breaches and prioritizing their IT security. All of those surveyed have implemented a number of measures and solutions to achieve this goal.

But there is no silver bullet: at present, respondents use an average of eight different security measures to protect against security breaches, with over half of IT decision-makers surveyed reporting that nine security measures are currently being used.

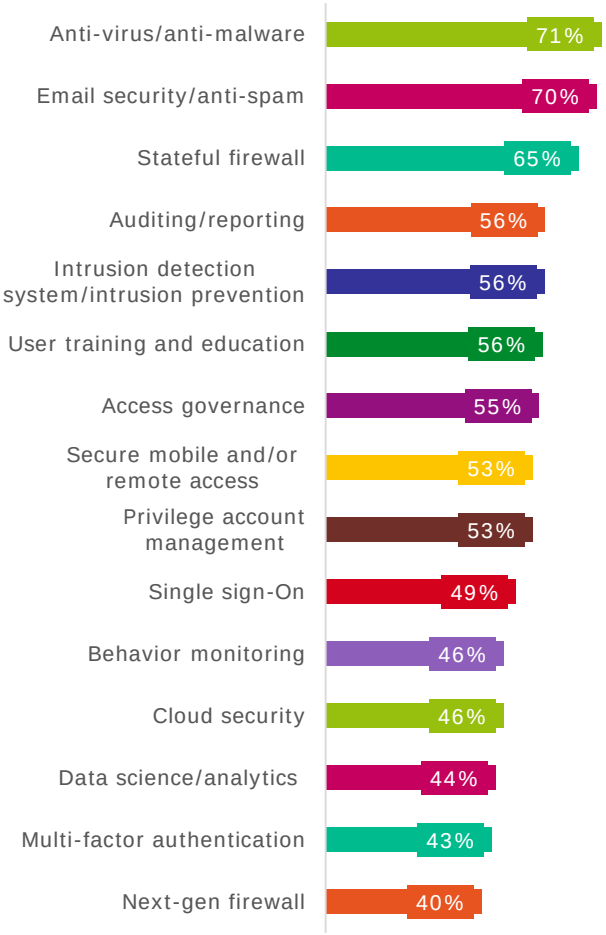

Figure 14: *Those who say that they are currently using the following security measures to help detect and/or prevent security breaches asked to all respondents (1440 respondents)*

Only 53% of organizations are currently using secure mobile and/or remote access security measures. Nearly half (47%) of respondent organizations may be leaving themselves exposed to unknown threats via vulnerabilities with BYOD or remote access usage.

Detecting a security breach

In general, IT decision-makers surveyed have confidence in their current security solutions, as more than four in five (83%) agree that their organization's current security processes enable them to identify a security breach immediately.

However, when prompted about their organization's latest breach in security, only 11% report that they were able to identify the source of the breach immediately. Moreover, only a fifth were able to detect the breach within the hour. On average it took respondent organizations seven hours to detect the source.

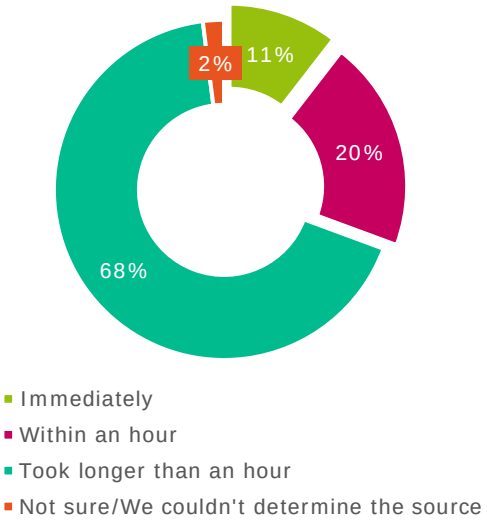

Figure 15: "For your last security breach, how quickly was your organization able to identify the source of the security breach?", *only asked to respondents who organization has experienced a security breach and the case of the breach was known (1237 respondents)*

There is a clear distinction between what IT decision-makers believe their IT solutions are capable of, and the reality of the situation. IT decision-makers therefore need educating about the potential limitations and improvements that can be made to the security measures their organizations have in place.

Once a breach has been detected, IT decision-makers surveyed suggest it *would* take their organization an average of six hours to take action. This is an average of an hour longer than respondents believe it *should* take with their current solutions. Almost half (48%) of

respondents believe that taking action following a breach *should* be achieved immediately or within the hour. This demonstrates that the IT security solutions of the majority (52%) are not as good as they require.

Experiencing a security breach

The ability to detect and then take action to resolve a security breach has become even more crucial, as 87% of respondent organizations have suffered a security breach at some point. 73% have experienced a breach in the last twelve months, over half of which occurring in the last six months.

Organizations are being attacked in a variety of different ways. There is no single root cause for these attacks experienced by the majority. Instead, organizations need to protect their perimeters against numerous sources and causes of security breaches.

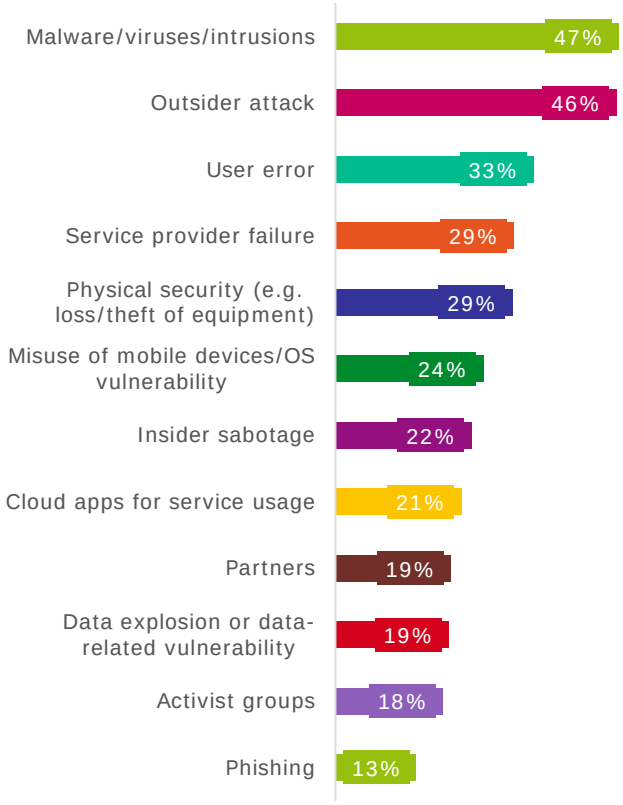

Figure 16: "What was the root cause of the security breaches your organization experienced?", *only asked to respondents that have experienced a security breach (1241 respondents)*

Vulnerabilities exposed by the misuse of mobile devices or operating systems are the root cause of a security breach, according to almost a quarter (24%) of IT decision-makers surveyed. This is a particular cause for concern, as 93% of those surveyed are allowing personal devices to access their organization's network; on average just over three in ten (31%) employees/end users take up the facility to access their organization's files via their personal devices.

Those who expect security to be their organization's top priority next year typically have more end users accessing the network via their personal devices. These organizations are recognising the need to prevent security breaches brought about by BYOD vulnerabilities; this is something other organizations are failing to do, which may open them up to greater threats, both known and unknown.

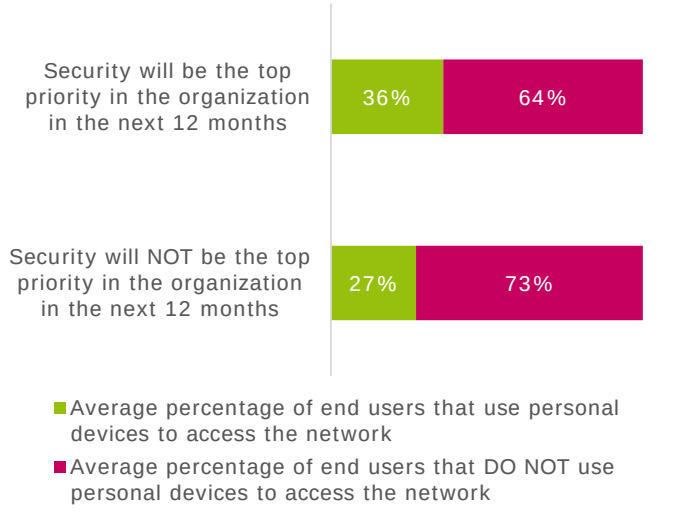

Figure 17: *Average percentage of end users that use personal devices to access the network, analyzed by whether security will be the organization's top priority next year*

Overall, security breaches have cost every respondent organization an average of a just under $1 million over the last twelve months. Despite these costs, many only prioritize IT security once they have fallen victim to a costly breach.

Respondents that expect security to be the top priority in their organization over the next twelve months have typically experienced higher costs resulting from a breach than the rest. On average the costs that these organizations have suffered over the last year have been $1.2 million, compared to losses of $660,000 for those not prioritizing security next year.

Figure 18: *Average amount of money that security breaches have cost organizations, analyzed by if security will be the top priority for the organization next year*

Organizations are not proactively preventing the consequences of poor security; instead they tend to commit resources once they have experienced a security breach and its costs first hand.

Protecting against cloud vulnerabilities

The use of cloud is extensive; more than nine in ten (91%) are already leveraging the cloud for their apps or data or are planning to. Using cloud has the potential to present vulnerabilities, which may expose a business to security threats. The use of cloud services has grown dramatically over the last few years. Have organizations invested in cloud security with equal enthusiasm?

At present, 46% of those surveyed are currently using cloud security. However 73% of respondents claim that their organizations are already using cloud. This means that only a little over half (54%) of cloud users do not have the security to match, leaving them exposed.

Respondents whose organizations intend security to be their top priority next year are more likely than others to be using cloud or be planning to do so.

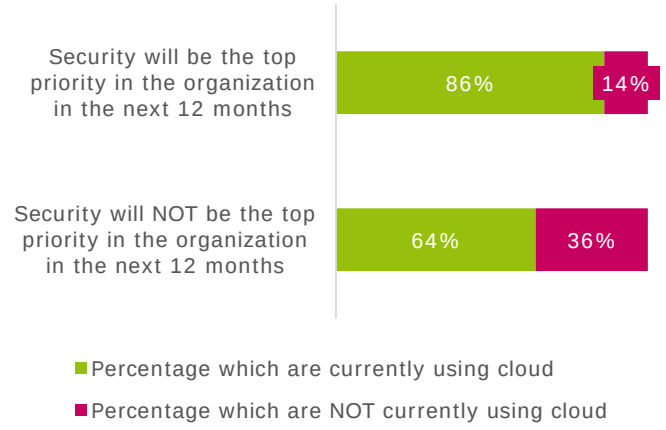

Figure 19: *Percentage of organizations which are using cloud, analyzed by if security will be the top priority for the organization next year*

As organizations increase their use of both cloud and BYOD, they will need to ensure that they have the security measures in place to protect themselves from any unknown threats. Some organizations are already recognising the link between increased adoption of these big trends innovations and their implication.

Country differences

Although the majority surveyed (83%) express confidence that their IT enables them to identify a security breach immediately, Australian respondents are the most confident as 92% believe that their systems have this ability. However, when asked about their latest security breach, Australian organizations took longer to detect the source than any other region in this study. The global average was seven hours to detect the breach, whereas Australian organizations took an average of ten hours.

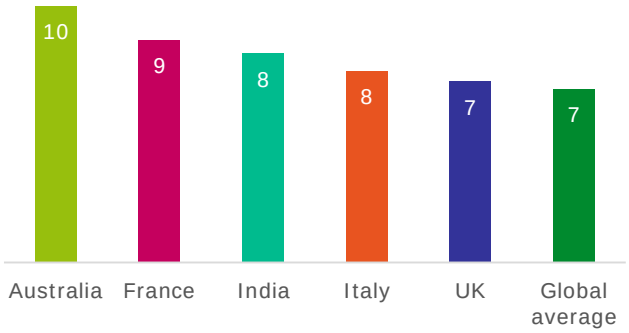

Figure 20: *Average amount of time in which the source of a security breach was able to be identified (in hours), analysed by regions which score higher than the global average*

More than four in ten respondents from the US claim that their organizations have been a victim of a security breach which was either caused by the misuse of mobile devices or operating system vulnerabilities (46%) or from cloud apps for service usage (43%). Respondents in the US claim that their organizations have suffered from these types of breach twice as often as the global average (24% and 21% respectively).

As figure 21 shows, organizations in this region have the highest proportion of end users accessing the network via their personal devices and the highest percentage of organizations currently using cloud.

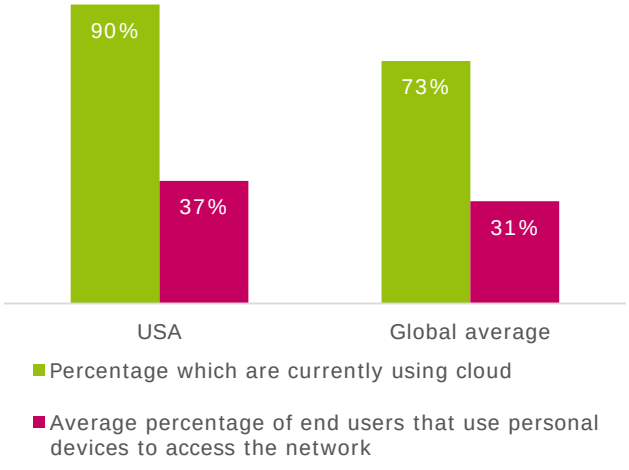

Figure 21: *Percentage of organizations which are using cloud, and average percentage of end users that use personal devices to access the internet, analyzed by region*

There is a strong correlation between a greater adoption of these big trends and the need for organizations to invest in security solutions in order to protect themselves against potential vulnerabilities.

Moreover, looking at all the regions, US respondent organizations have suffered the highest costs from security breaches on average; an average of almost $1.5millon, $600,000 more than the global average.

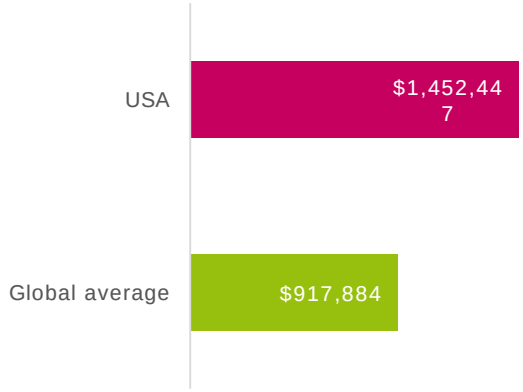

Figure 22: *Average amount of money that security breaches have cost organizations, analyzed by region*

Understanding of threats

Have IT decision-makers learnt from security breaches and are they now able to protect their organizations from threats? The research suggests that they are at least attempting to keep on top of the latest developments; respondents say that they typically use three sources to keep up to date with security threat analysis and best practices. Over half of respondents use internal research/their own intelligence (60%) and external research/industry news (55%).

A quarter or more (25-27%) of respondents are not confident that their solutions can protect the organization from threats from both inside and outside the company. However, they display more confidence if their organization has suffered high costs as a consequence of a security breach; this chastening experience typically causes an upsurge in spending to prevent a repetition.

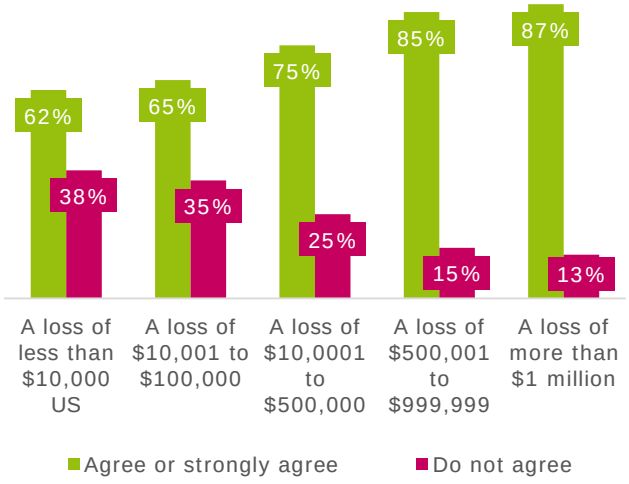

Figure 23: *To what extent respondents agree that their current solutions are adequately protecting them from threats that originate both inside and outside the organization, analyzed by how much security breaches have cost the organization in the last twelve months (973 respondents)*

This degree of confidence from IT decision-makers suggests that they have learnt from breaches and implemented solutions as a result as opposed to having them in place beforehand. They are implementing a retrospective fix, not proactively implementing preventative measures.

Protecting the organization both inside and outside the perimeter

Just over three-quarters (76%) of respondents agree that, in order to combat today's criminal, an organization must protect itself both inside and outside its perimeter. In order to achieve this, 64% agree that organizations will need to restructure/re-organize their IT processes and collaborate more with other departments. Doing so will enable them to stay ahead of the next security threat.

Despite this confidence, 64% of IT decision-makers surveyed fear that they cannot fully protect their organization from a breach, agreeing that it is not a matter of *if* a company will be breached, but *when*.

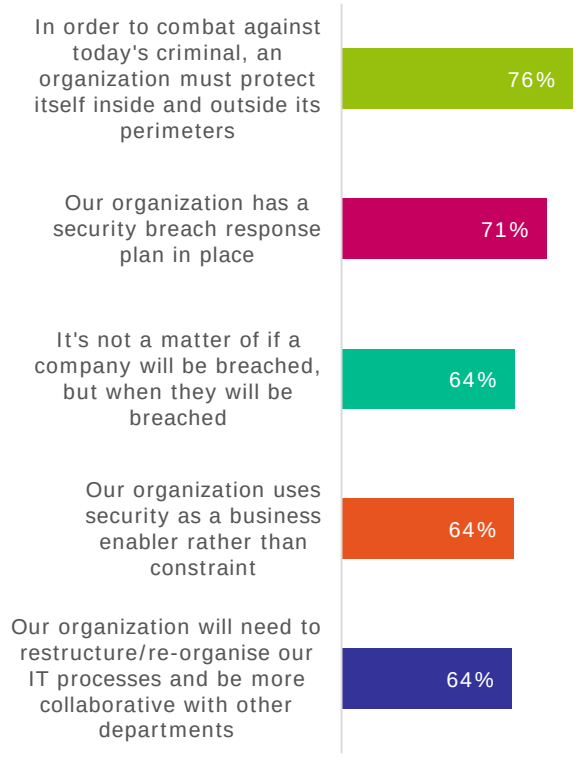

Figure 24: Those selecting agree or strongly agree for "To what extent do you agree or disagree with the following statements?" *asked to all respondents (1440 respondents)*

Almost three in ten (29%) do not have a security breach response plan in place, should a breach occur. Although they may be expecting a breach

on the balance of probabilities, they are not prepared should one to happen. As many organizations either do not have solutions which immediately detect a breach or lack the ability to react quickly, they are likely to suffer greater costs and overall losses to the organization.

Although IT decision-makers surveyed recognize what they need to do to protect their organization's perimeter, they are not confident that they have the capability to do so at present. Therefore many will need guidance and support to achieve what they know their organizations need.

Country differences

Those surveyed from US organizations are most anxious about security breaches, in comparison to other regions in this study.

Figure 25: Those selecting agree or strongly agree for "To what extent do you agree or disagree with the following statements?" *analyzed by region*

Over four in five (86%) respondents in the US believe it is not a matter of *if* a company will be breached, but *when* it will be breached. This is 20% higher than the global average. Furthermore, significantly more IT decision-makers surveyed in the US believe that their organizations will need to protect themselves both inside and outside its perimeters (93% compared to the global average of 76%), and they accept that their organizations will need to restructure/re-organize their IT processes (85% versus 64%).

Organizations in the US are increasing collaboration in order to stay ahead of the next security threat, although they expect to become a victim of a breach at some point. High costs resulting from breaches ($1.45 million) are likely to have increased their fears and their desire to protect themselves.

Conclusion

IT security is crucial; organizations need to protect themselves from both insider and outsider attacks. Enterprises are spending an average of 17% of their IT budget on IT security. This focus on security is set to increase in the near future, as 86% of IT decision-makers surveyed report that their organizations will be prioritizing security over the next twelve months.

However, expenditure alone is not necessarily protecting them. During the past year, security breaches have cost respondent organizations an average of almost $1 million each. Furthermore, organizations are more likely to prioritize and commit resources to prevent breaches *after* they become a victim. Those who are now prioritizing security have suffered costs of $1.2 million, whereas those not prioritizing security have incurred average costs of $660,000, suggesting that greater loss is putting security front of mind. The failure to take a proactive approach is leaving organizations vulnerable to attack. Organizations that learn from others' mistakes and proactively protect themselves now are likely to save on costs in the future.

Unknown threats could prove costly for organizations. 64% have resigned themselves to the fact that it is not a matter of *if* they will be breached, but *when*.

Cloud usage and BYOD bring with them the potentially unknown vulnerabilities that could lead to security breaches. 91% of those surveyed are already hosting the cloud for their apps or data or are planning to, and 93% facilitate the use of personal devices to access their networks. However, only a minority of these organizations have implemented cloud security (46%) or policies for BYOD security (44%). This highlights a troublesome gap between the many that are using cloud and BYOD and the comparative few that are protecting themselves from unknown threats that could come through these channels. They are leaving themselves exposed.

The research suggests the choice for those yet act is clear: do so now in order to protect the company's perimeters, or risk a significant cost later.

About Dell:

Dell Inc. listens to customers and delivers innovative technology and services that give them the power to do more. For more information, visit www.dell.com

About Vanson Bourne:

Vanson Bourne is an independent specialist in market research for the technology sector. Our reputation for robust and credible research-based analysis, is founded upon rigorous research principles and our ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com