



THE GFI SOFTWARE SMB AND IT SECURITY REPORT

September 2009



Executive Summary

Compared to 2008, small and medium businesses (SMBs) are more likely to have higher IT budgets in 2009 than they are to have stagnant or reduced budgets.

Just over one-third (37%) of SMBs indicated that their overall 2009 budget is either slightly higher or significantly higher than it was in 2008, which is more than those who said it is at the same level (33%) or who said it was slightly or significantly reduced (25%).

If the recession is prolonged and IT budgets are forced to be cut, IT security will be spared. One in five SMBs indicates that it is not likely that IT security will be the first to be cut, twice the number who say it is likely their IT security will be the first cut.

In total, 21% of SMBs state that they are less likely to cut spending on IT security than on other projects if the recession is prolonged and IT budgets are forced to be cut. This is more than twice as many (9%) who indicate that they are more likely to cut spending on IT security than on other projects. Thirty-eight percent (38%) indicate that they are neither more nor less likely to cut spending on IT security than any other area; 21% state that spending on IT security is minimal anyway, so there is no real scope for further cuts, and 11% say IT is vital to maintain a high level of investment in IT security as a key priority.

The IT security threats that most concern SMBs are accidental data corruption, malware attacks, and external hacking.

Overall, SMBs do not appear to be too concerned about various IT security threats. Of 11 common IT security threats, only two threats concerned at least half of the SMBs.

- » Fifty-three percent (53%) of SMBs said they are “extremely” or “very concerned” about accidental data corruption.
- » Fifty-one percent (51%) of SMBs said that Web-borne malware attacks concern them.

However, SMBs are overwhelmingly more concerned about external security threats than they are internal threats.

Two-thirds (67%) of SMBs report they are more concerned about external security threats, compared to just 9% who say they are more concerned about internal threats. One quarter (24%) indicate they are equally concerned about both external and internal security threats.

A majority of SMBs have some sort of IT security software applications in place to help guard against security threats.

E-mail anti-virus software is the most common form of IT security software application that SMBs use, with 94% indicating they currently possess the software, including 13% who indicate they are planning on boosting their e-mail virus software capabilities. SMBs are least likely to use portable storage device network access management software, with 56% of SMBs indicating they currently use this type of IT security application (15% plan on boosting capabilities).

A majority of SMBs have security policies in place regarding Internet use, but far fewer have the means to monitor and/or filter the HTTP traffic.

Six out of ten (61%) SMBs indicate they have policies in place regarding Internet use, but less than half (47%) say they have the means to monitor and/or filter traffic. However, 15% of SMBs indicate they are considering adding monitoring and/or filtering capabilities, and an additional 5% said implementation is planned.

Similarly, a majority of SMBs have a formal policy on restricting access to sensitive data, but fewer have a policy to categorize company data according to its sensitivity.

Almost six in ten (58%) SMBs have a formal policy on restricting access to sensitive data. An additional 11% say developing a formal policy is under consideration. Less than half (47%) of SMBs say they have a formal policy in place to categorize company data according to its sensitivity, and an additional 14% indicate developing a formal policy is under consideration.

Additionally, few SMBs have rules or policies governing e-mail storage or retention.

Slightly more than one-third of SMBs have rules stating where e-mails should be stored (37%) or how long copies of e-mails must be held (35%). However, 18% of SMBs that currently do not have rules stating where e-mails should be stored are planning on creating rules, as are 20% of SMBs that currently do not have rules stating how long copies of e-mails must be held.

SMBs that use Web filtering software are most likely to use the software as a form of security, to prevent illegal and/or unacceptable Web browsing and to manage and control Internet usage.

Two-thirds (67%) of SMBs that use Web filtering software use the software as a form of security against virus and malware downloads. Over half use the software to prevent illegal and/or unacceptable Web browsing (55%) and to manage and control Internet usage (51%). SMBs are least likely to use Web filtering software to create customized browsing rules for groups or for dynamic policy changes on the fly.

Twice as many SMBs use hosted/managed services than do not. And of those who use these services, no single set-up dominates.

Fifty-five percent (55%) of SMBs stated that they use one or more hosted/managed services, while 27% indicate they do not use any hosted/managed services. The remainder are either considering (2%) using hosted/managed services or do not know if they use any (16%). Of the SMBs that use at least one hosted/managed service, 29% state that the services are used for minor applications, 24% are used for security applications, and 21% are used for CRM/ERM systems. The remaining SMBs use the services for network monitoring or for redundancy.

Among the cloud models in use today, more SMBs are likely to exploit a full on-line, on-demand model than managed service or a hybrid model.

Three out of ten (29%) SMBs indicate that the full on-line, on-demand cloud model applies to their situation, and another 29% replied that they use a mix of the three models – full on-line, on-demand; managed services; and hybrid model. Further, 27% state they use the managed service model, and 15% use the hybrid model.

Easy Internet access and scalability are the top two advantages that SMBs see for using hosted services.

SMBs rated easy Internet access and scalability as the top advantages of using hosted services rather than an on-premise software solution. The advantages associated with SaaS vendors (expertise and accountability) were rated as the least advantageous reasons for using hosted services.

Application performance, data privacy, and systems failure are the biggest concerns of SMBs in using hosted services.

Between 62% and 64% of SMBs indicated that application performance, systems failure/redundancy, and data privacy/security are of high or very-high concern when using hosted services. These three areas received the highest concern. On the other end, SMBs are least concerned about vendor lock-in or complex pricing models, where a little over one-third indicated these areas were of high or very-high concern.

More than half of SMBs indicate they would prefer a vendor that gave them the option to easily switch models as their business requirements changed.

Just over half (52%) of SMBs would prefer a vendor that gave them the option to easily switch models as their business requirements changed, which is almost five times as many who said they would not prefer a vendor who provided that option (11%). Just over one-third (37%) indicated that they were unsure if they would or would not prefer a vendor who provided this option.

Objectives and Methodology

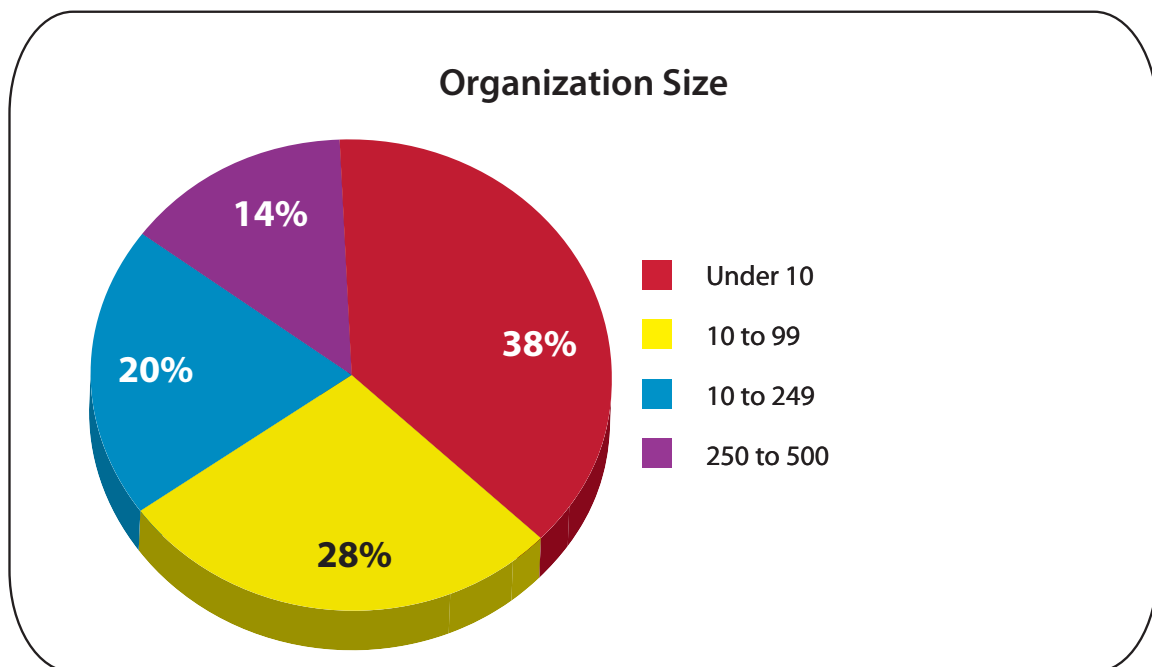
This report presents the findings of an online survey conducted among 540 IT professionals based in the United States for the purposes of:

- » Assessing the “readiness” of the small and medium businesses (SMBs) in the U.S. to deal with security issues
- » Determining how priorities in IT security have changed in the SMB market due to the current economic environment

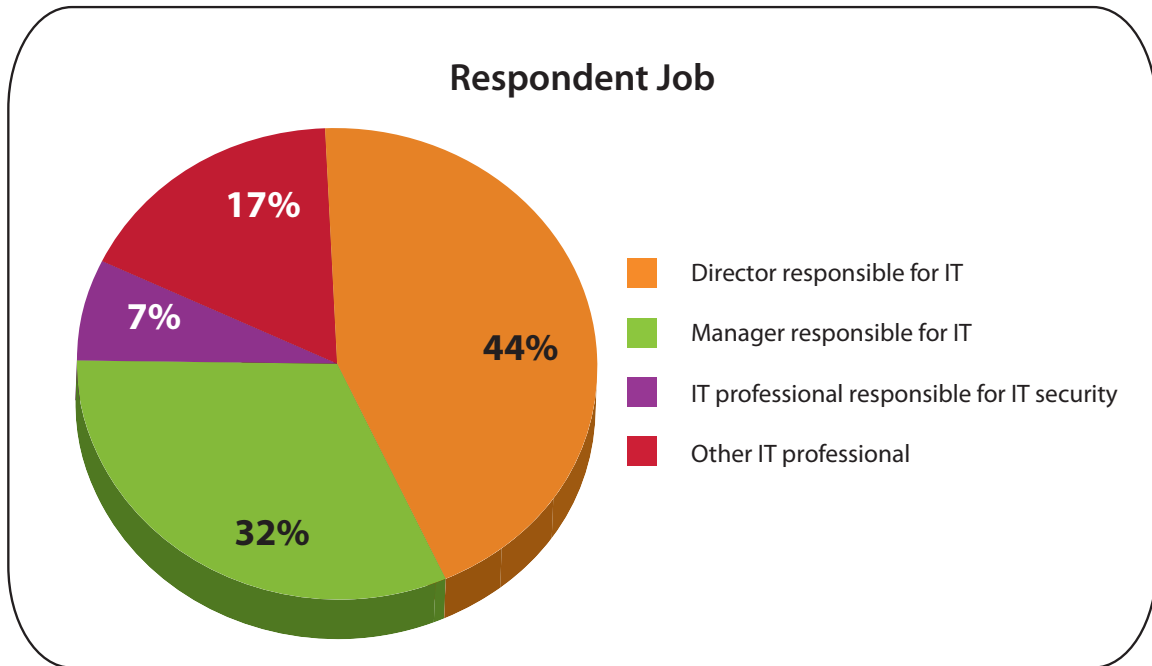
The survey was sent to 19,067 members on an IT panel managed by e-Rewards. The panel, comprised of approximately 250,000 members, is representative of a large number of IT professions/titles, including CIOs. Interviewing for this survey was completed during the period July 27 through August 6, 2009. Participants were screened to ensure they met the following criteria:

1. IT professional with decision-making authority or specific responsibility for IT security
2. Work at a small- or medium-sized enterprise that has 500 or less employees

Two-thirds (66%) of the survey respondents work at a company that has less than 100 employees, with 38% working at a company with less than 10 employees.



Three-fourths (76%) of the survey respondents are directors or managers with IT responsibility and/or decision-making authority.

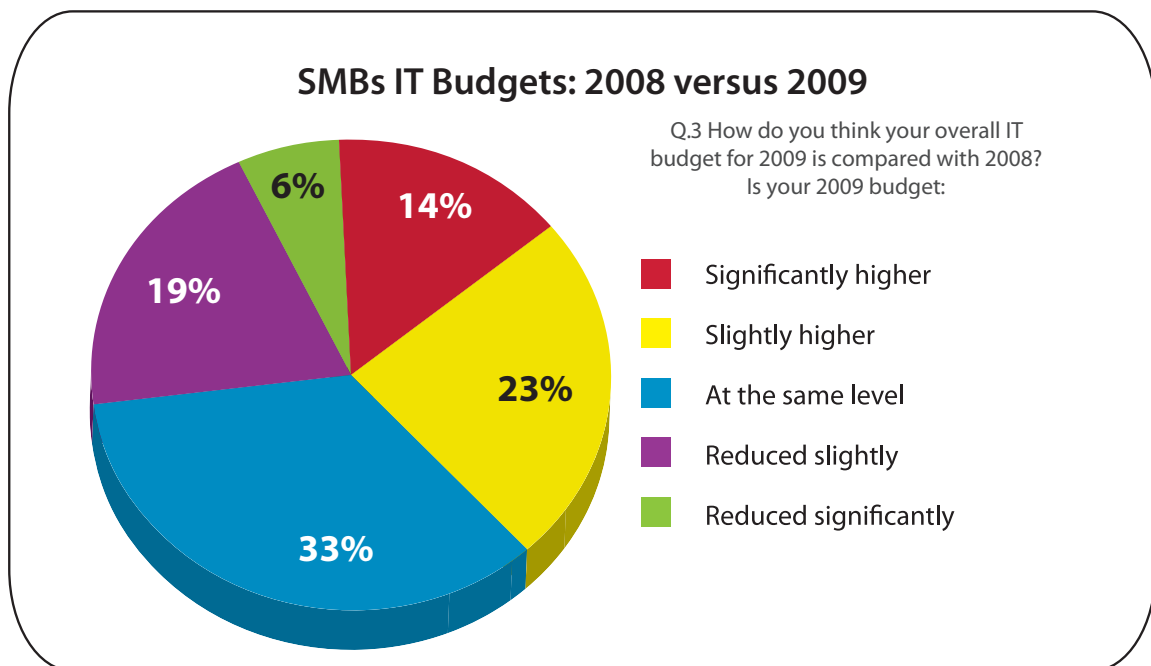


Key Findings

IT Budget Trends

Compared to 2008, small and medium enterprises (SMBs) are more likely to have higher IT budgets in 2009 than they are to have stagnant or reduced budgets.

IT professionals were asked if they thought the overall IT budget for 2009 would be higher, lower, or about the same as it was for 2008. Just over one-third (37%) of SMBs indicated that their overall 2009 budget is either slightly higher or significantly higher than it was in 2008, which is more than said it is at the same level (33%) or who said it was slightly or significantly reduced (25%).



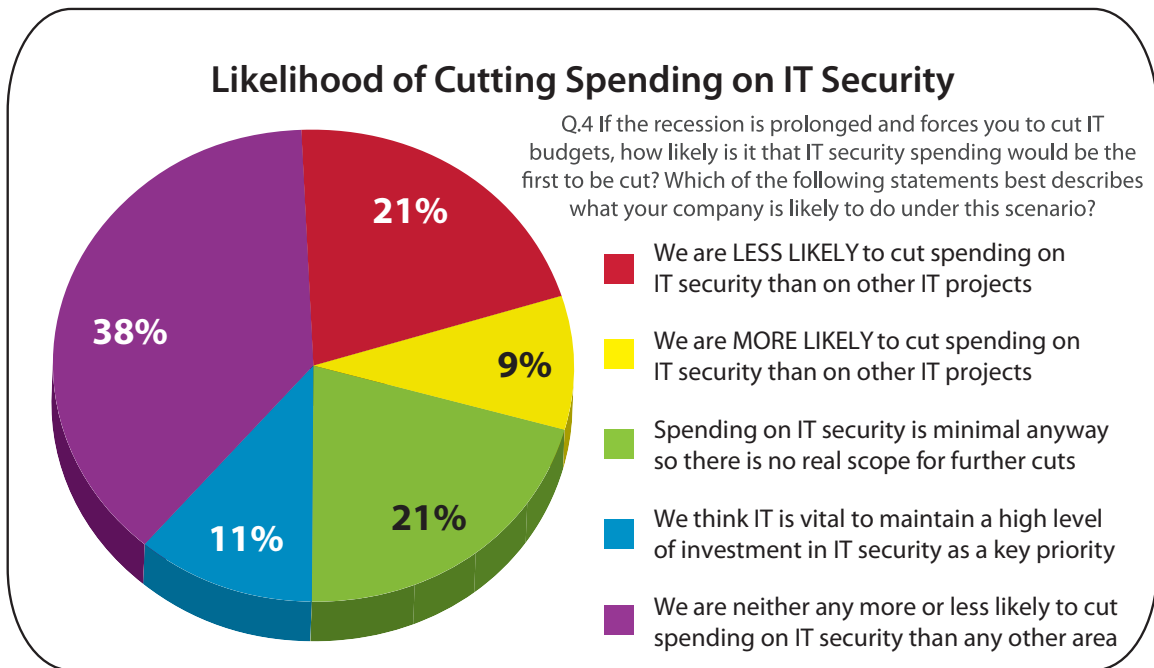
Company size appears to have some bearing on the likelihood that 2009 IT budgets are higher than they were in 2008. Businesses with at least 100 employees are slightly more likely to report higher budgets than companies with less than 100 employees, but the difference is not statistically significant.

Table 1
Q.3 How do you think your overall IT budget for 2009 is compared with 2008?

	Number of Employees					
	<10	10-99	Less than 100 (net)	100-249	250-500	100+(net)
Higher IT budget	35%	35%	35%	42%	38%	41%

If the recession is prolonged and IT budgets are forced to be cut, more SMBs indicate that it is not likely than it is likely that IT security will be the first to be cut.

Less than one in ten (9%) SMBs indicates that they are more likely to cut spending on IT security than on other projects if the recession is prolonged and IT budgets are forced to be cut. This compares to one-fifth (21%) of the SMBs that report that they are less likely to cut spending on IT security than on other projects. Coupled with the 21% who state that spending on IT security is minimal anyway so there is no real scope for further cuts, and the 11% that say IT is vital to maintain a high level of investment in IT security as a key priority, a total of 53% of SMBs indicate that even with additional cuts in IT budgets, IT security will likely survive further reduction.

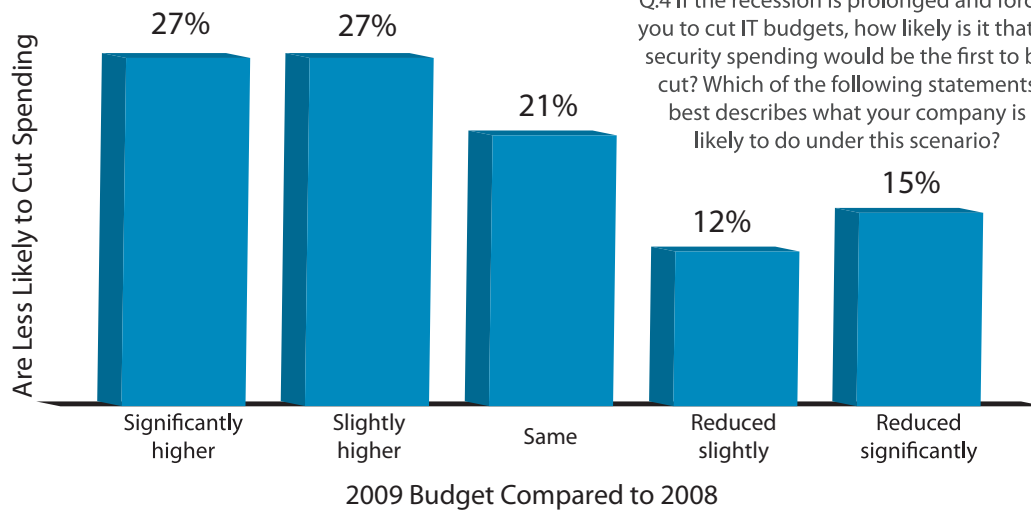


Differences in budget strategy exist for businesses based on the number of employees they have. For example, companies with 250-500 employees are the most likely of the businesses to say that IT is “vital,” while businesses with less than 10 employees are the most likely to report that spending on IT security is “minimal.”

Table 2 Q.4 If the recession is prolonged and forces you to cut IT budgets, how likely is it that IT security spending would be the first to be cut? Which of the following statements best describes what your company is likely to do under this scenario?				
	Number of Employees			
	<10	10-99	100-249	250-500
We think IT is vital to maintain a high level of investment in IT security as a key priority	9%	12%	9%	14%
We are less likely to cut spending on IT security than on other IT projects	16%	21%	31%	23%
We are more likely to cut spending on IT security than on other IT projects	5%	14%	11%	5%
Spending is minimal on IT security anyway, so there is no real scope for further cuts	30%	17%	12%	17%

Noteworthy is that SMBs with higher budgets in 2009 are less likely to cut spending on IT security (i.e., higher budgets mean lower probability of cuts, while lower budgets mean higher likelihood of cuts).

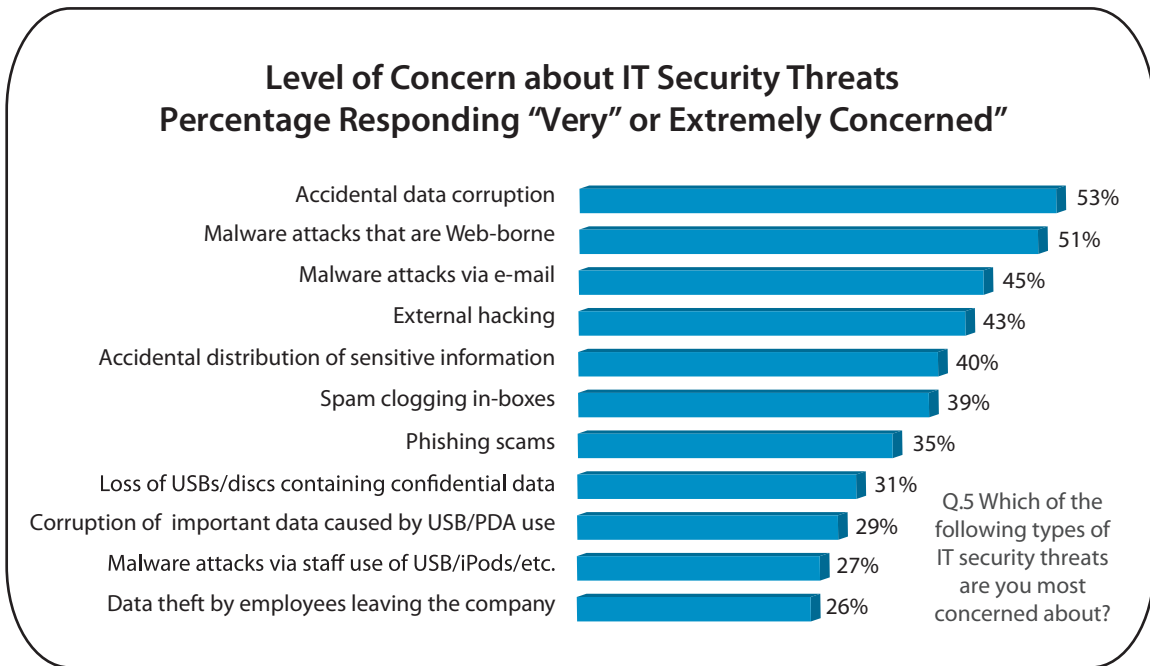
Percentage of SMBs That Are Less Likely to Cut Spending on IT Security



IT Security Risks

The IT security threats that most concern SMBs are accidental data corruption, malware attacks, and external hacking.

Overall, SMBs do not appear to be too concerned about various IT security threats. Of 11 common IT security threats, only two threats concerned at least half of the SMBs. Of particular interest, given the explosive growth in portable devices, is how unconcerned companies appear to be with malware attacks via staff use of USBs, iPods, etc. Four in ten (40%) respondents stated they are “not that concerned” with this type of threat, and three-fourths (73%) are only “somewhat concerned” or “not that concerned.”



SMBs are much more concerned about employees accidentally corrupting or distributing data than they are of employees stealing data. Nine out ten (90%) SMBs are at least somewhat concerned about accidental data corruption, and three-fourths (76%) are at least somewhat concerned about accidental distribution of sensitive information. Yet almost half (46%) of SMBs indicate that they are “not that concerned” about data theft by employees leaving the company.

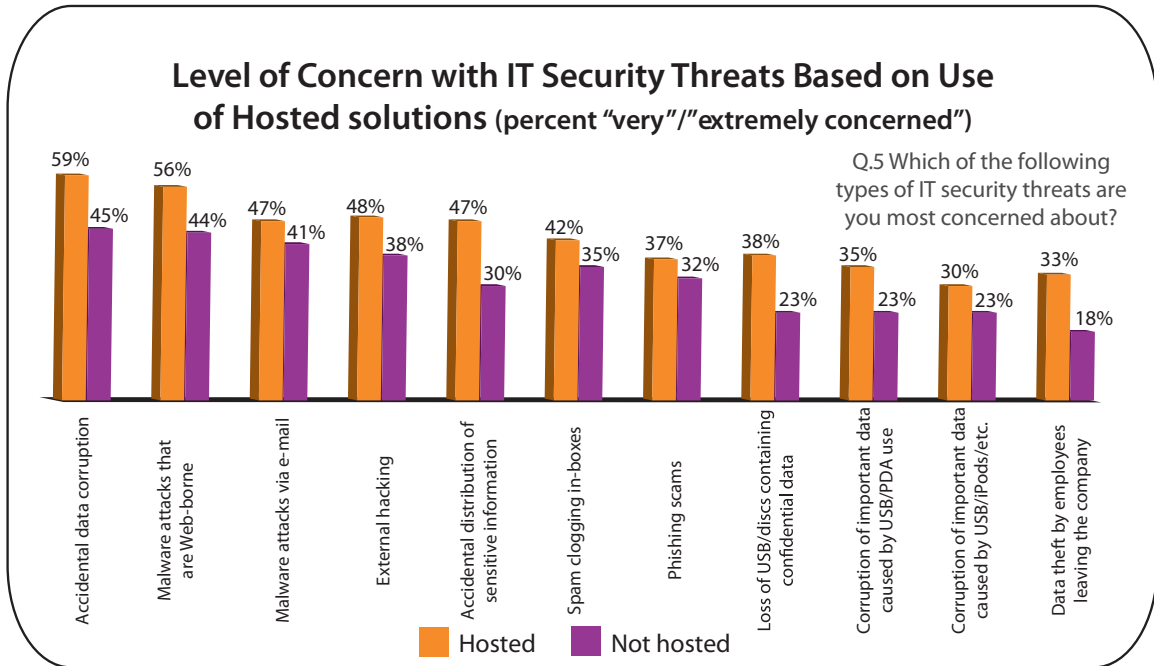
Overall, larger SMBs tend to be more concerned about IT security threats than smaller SMBs. For example, SMBs with 100 or more employees are more likely than smaller SMBs (less than 100 employees) to be concerned with security threats associated with USBs, iPods, and PDAs as well as data theft from employees leaving the company.

Table 3
Q.5 Which of the following types of IT security threats are you most concerned about?

(Percent "very"/"extremely concerned")	<100 employees	100+ employees
Accidental data corruption	54%	52% (-2%)
Phishing scams	35%	34% (-1%)
Malware attacks via e-mail	44%	46% (+2%)
External hacking	42%	46% (+4%)
Malware attacks that are Web-borne	49%	55% (+6%)
Spam clogging in-boxes	37%	43% (+6%)
Corruption of important data caused by USB/PDA use	27%	35% (+8%)
Loss of USBs/discs containing confidential data	27%	38% (+11%)*
Malware attacks via staff use of USBs/iPods/etc.	22%	38% (+13%)*
Data theft by employees leaving the company	22%	35% (+13%)*
Accidental distribution of sensitive information	34%	50% (+16%)*

*Statistically significant at 95%

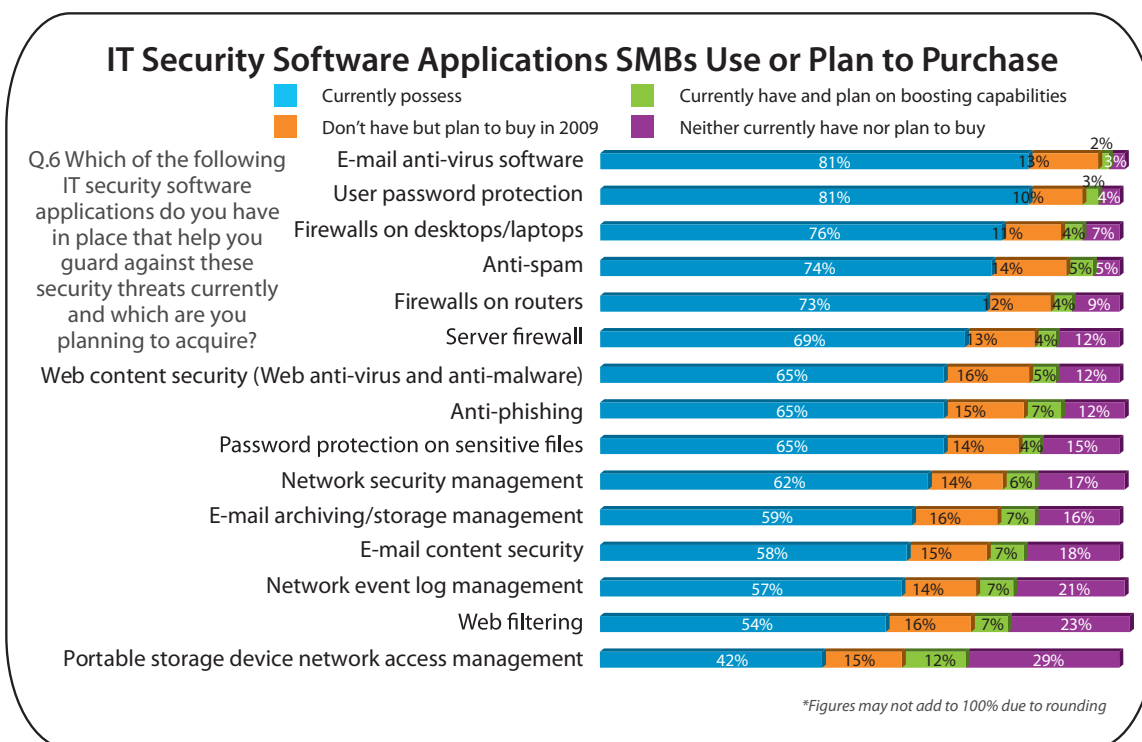
SMBs using hosted solutions tend to be more concerned about IT security threats than companies that do not use hosted solutions.



A majority of SMBs have some sort of IT security software application in place to help guard against security threats.

E-mail anti-virus software is the most common form of IT security software application that SMBs use, with 94% indicating they currently possess the software, including 13% who indicate they possess the software and plan to boost their e-mail virus software capabilities. Additionally, use of firewalls is fairly common among SMBs, with over 80% using some form of firewall.

SMBs are least likely to use portable storage device network access management software, with 56% of SMBs indicating they currently use this type of IT security application (15% plan on boosting capabilities).



Also noteworthy is that one quarter (25%) of SMBs do not currently check what content is leaving their company (i.e., percent lacking e-mail content security applications).

SMBs are more likely to have **firewalls** on the desktops and laptops than they are on the routers and servers.

- » SMBs with less than 10 employees are most likely to have firewalls on the desktops/laptops.
- » SMBs with between 10-99 employees are most likely to have firewalls on the routers.
- » SMBs with between 250-550 employees are most likely to have firewalls on the servers.

SMBs are more likely to have **e-mail** anti-virus software than they are e-mail archiving/storage management and e-mail content security.

SMBs are more likely to have general **password** protection than they are to have password protection on sensitive files.

SMBs are more likely to have **Web** content security than they are Web filtering.

- » SMBs with less than 10 employees are most likely to have Web content security.
- » SMBs with between 250-550 employees are most likely to have Web filtering software.

SMBs are more likely to have **network** security management than they are network event log management.

SMBs are more likely to have anti-spam software than they are anti-phishing software.

Overall, SMBs that are more concerned about external security threats are more likely than SMBs that are more concerned with internal threats to have IT security software applications. The exceptions, however, have to do with Web applications.

- » SMBs which are more concerned about internal threats are more likely to use Web filtering software.
- » SMBs which are more concerned about internal threats are about as likely as SMBs that are more concerned about external threats to use Web content security.

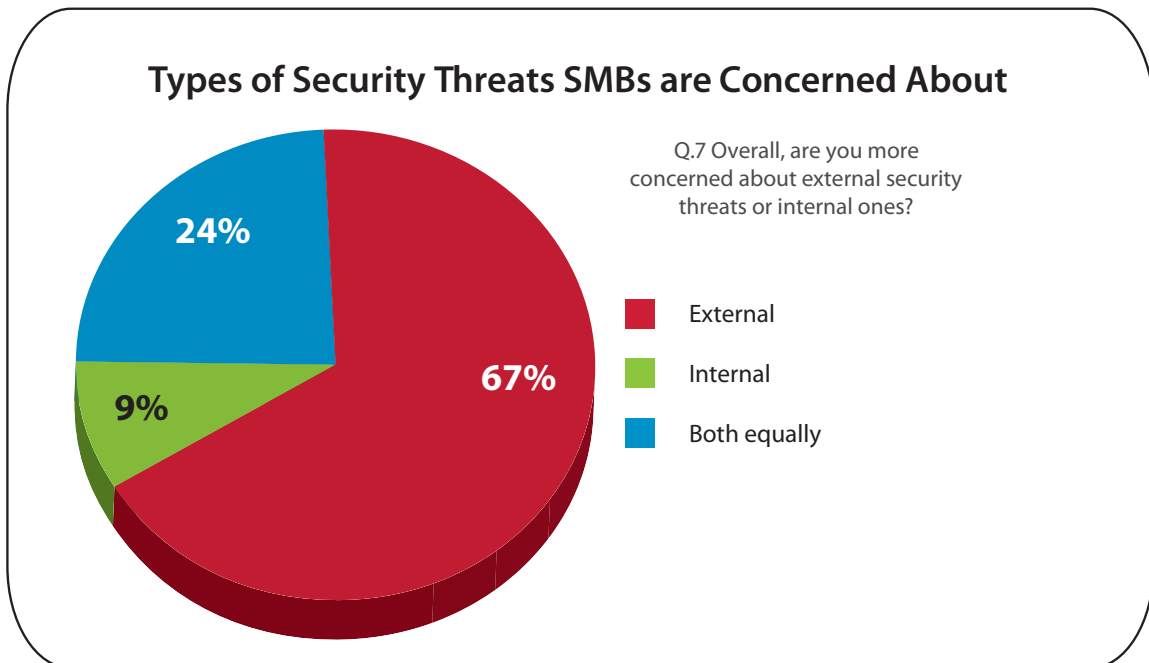
SMBs that do not use hosted services are more likely to use IT security software applications. However, SMBs that do use hosted services are more likely to use the following types of applications:

- » Password protection on sensitive files
- » Network security management
- » Network event log management
- » Web filtering
- » Portable storage device network access management

The higher incidence of use of the above security software applications by SMBs that use hosted services may indicate what types of security threats these businesses are more concerned with.

SMBs are overwhelmingly more concerned about external security threats than they are about internal threats.

Two-thirds (67%) of SMBs report they are more concerned about external security threats, compared to just 9% who say they are more concerned about internal threats. One quarter (24%) indicate they are equally concerned about both external and internal security threats.



Larger SMBs are more concerned with internal threats, such as data theft, than are smaller SMBs that are more concerned with viruses and hacking attacks.

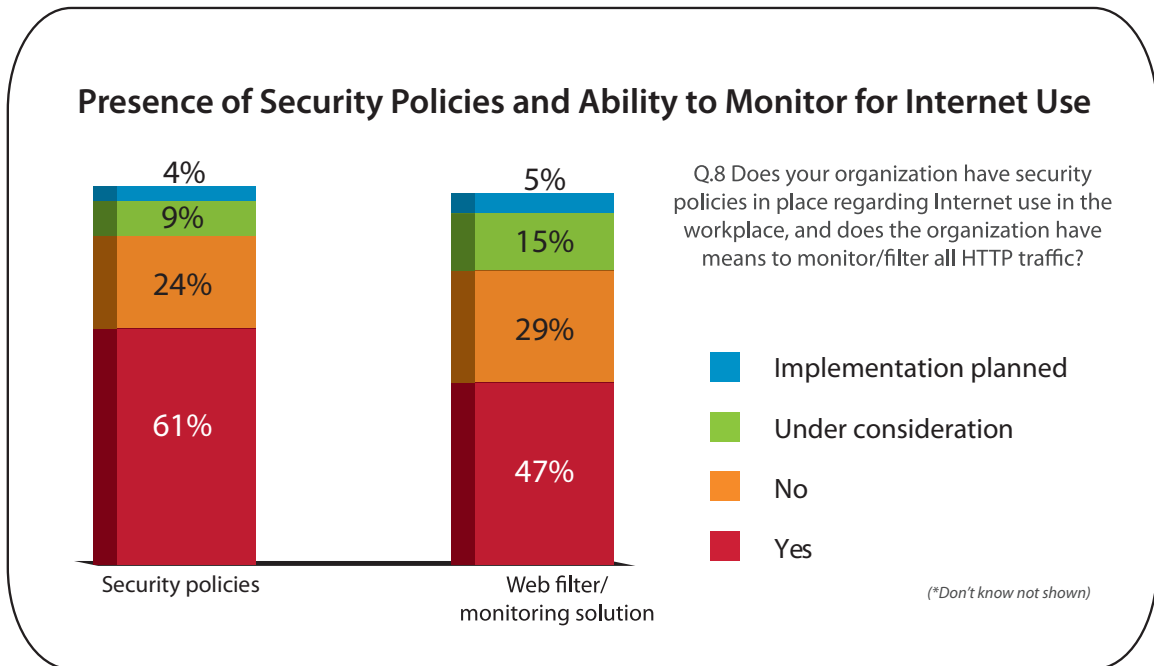
Table 4
Q.7 Overall, are you more concerned about external security threats or internal ones?

	Number of Employees			
	<10	10-99	100-249	250-500
Internal threats	5%	7%	11%	22%
External threats	76%	70%	54%	50%

Internet Usage

A majority of SMBs have security policies in place regarding Internet use, but far fewer have the means to monitor and/or filter the HTTP traffic.

Six out of ten (61%) SMBs indicate they have policies in place regarding Internet use, but less than half (47%) say they have the means to monitor and/or filter traffic. However, 15% of SMBs indicate they are considering adding monitoring and/or filtering capabilities, and an additional 5% said implementation is planned.



Larger SMBs are much more likely to have policies in place regarding Internet use as well as the means to monitor/filter HTTP traffic.

Table 5
Q.8 Does your organization have security policies in place regarding Internet use in the workplace, and does the organization have the means to monitor/filter all HTTP traffic?

(Percent "Yes")	Number of Employees			
	<10	10-99	100-249	250-500
Policies	42%	66%	74%	83%
Web monitoring solution	26%	51%	61%	72%

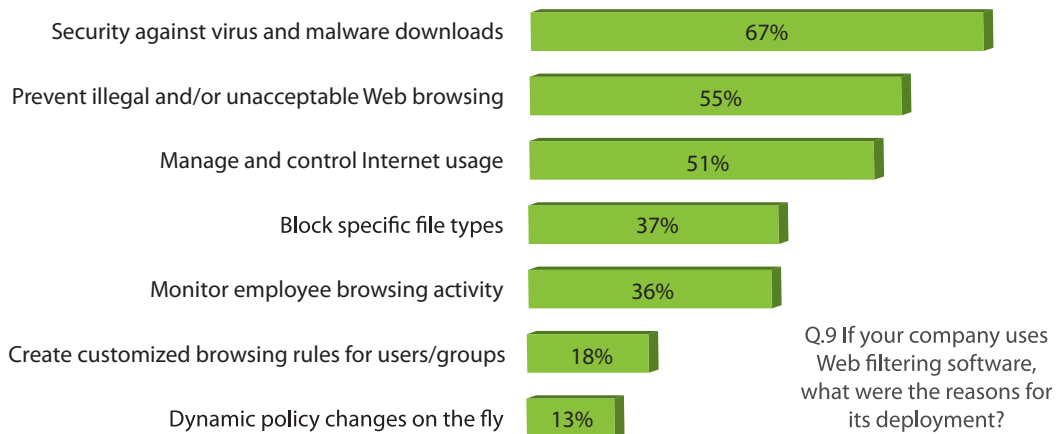
Similarly, SMBs that are more concerned with internal threats than external threats are more likely to have security policies in place and the ability to monitor Internet traffic.

SMBs that use hosted services are also more likely than SMBs that don't use hosted services to have policies in place and the means to monitor traffic.

SMBs that use Web filtering software are most likely to use the software as a form of security, to prevent illegal and/or unacceptable Web browsing and to manage and control Internet usage.

Two-thirds (67%) of SMBs that use Web filtering software use the software as a form of security against virus and malware downloads. Over half use the software to prevent illegal and/or unacceptable Web browsing (55%) and to manage and control Internet usage (51%). SMBs are least likely to use Web filtering software to create customized browsing rules for groups or for dynamic policy changes on the fly.

Reasons for Using Web Filtering Software

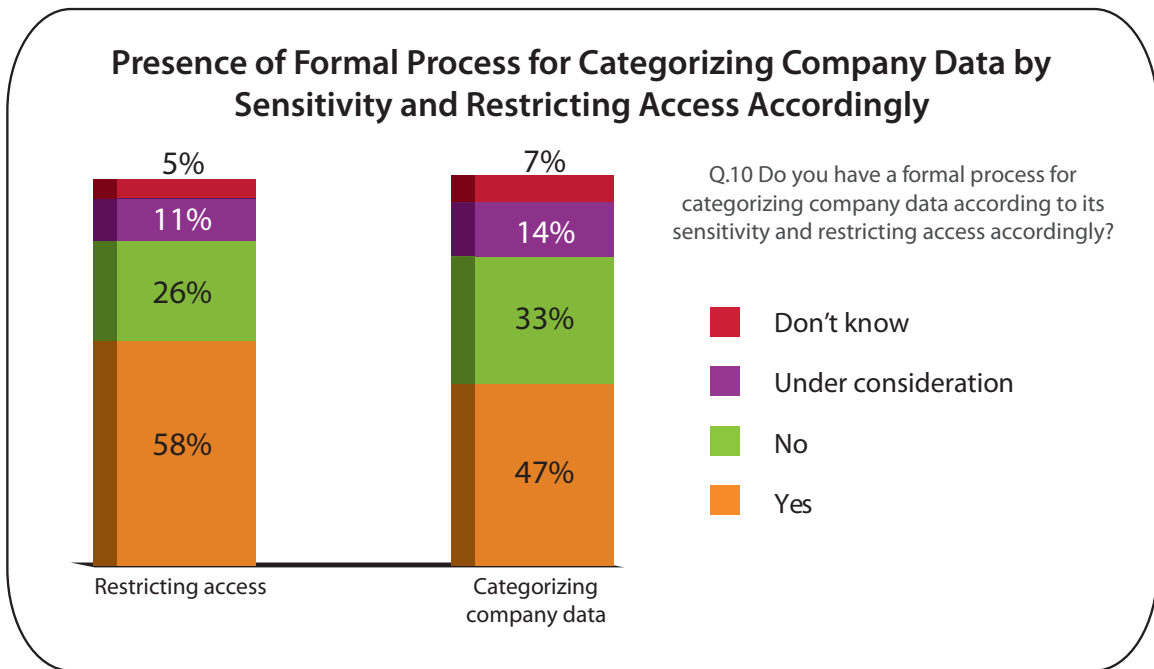


**Exceeds 100% because multiple answers can be selected*

Sensitive and Confidential Information

A majority of SMBs have a formal policy on restricting access to sensitive data, but fewer have a policy to categorize company data according to its sensitivity.

Almost six in ten (58%) SMBs have a formal policy on restricting access to sensitive data. An additional 11% say developing a formal policy is under consideration. Less than half (47%) of SMBs say they have a formal policy in place to categorize company data according to its sensitivity, and an additional 14% indicate developing a formal policy is under consideration.



Similar to the finding that larger SMBs are much more likely to have policies in place regarding Internet use as well as the means to monitor/filter HTTP traffic, larger SMBs are also more likely to categorize company data according to its sensitivity and restrict access to that data.

Table 6
Q.10 Do you have a formal process for categorizing company data according to its sensitivity and restricting access accordingly?

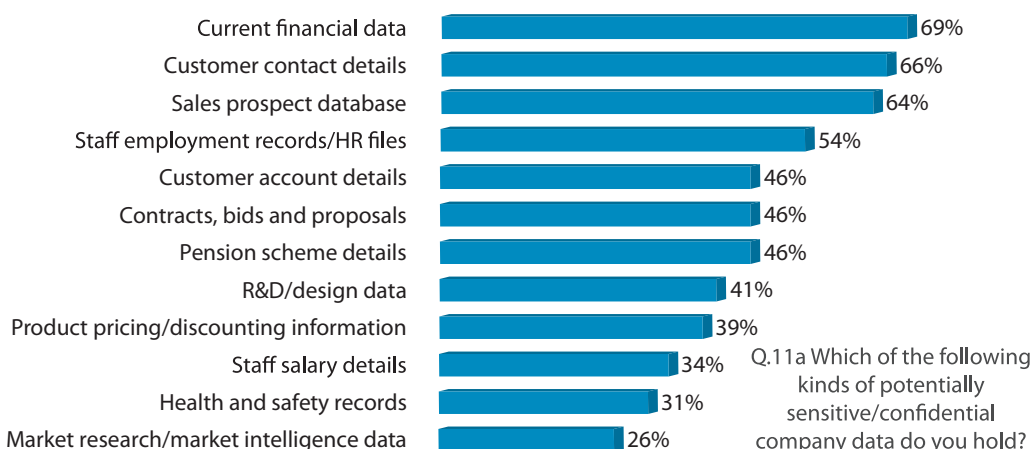
(Percent "Yes")	Number of Employees			
	<10	10-99	100-249	250-500
Restricting access	44%	59%	71%	73%
Categorizing data	40%	49%	49%	55%

SMBs that use hosted services are also more likely to categorize company data according to sensitivity and restrict access accordingly.

Virtually all SMBs indicate that they hold sensitive or confidential data, with current financial data being the most common form of sensitive or confidential data held.

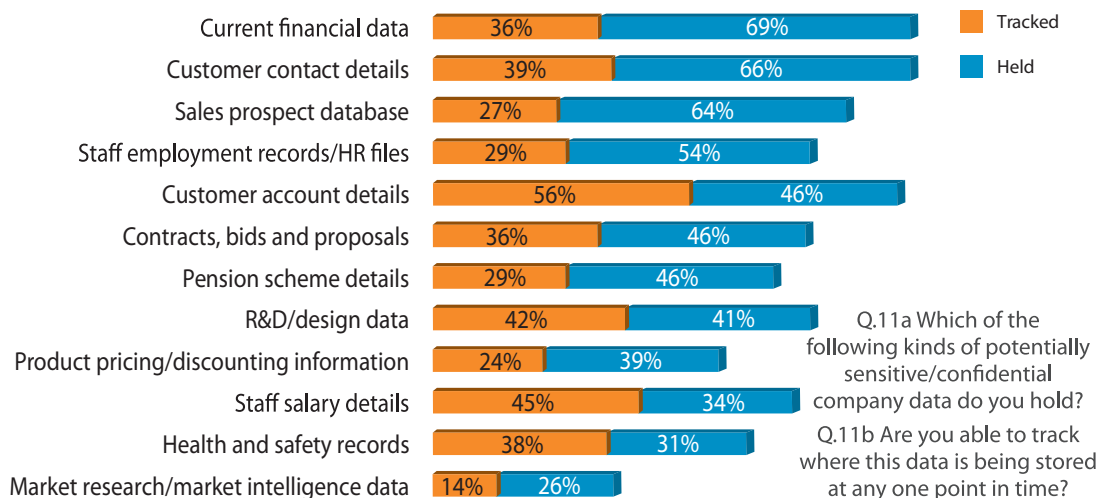
Virtually all (98%) of the SMBs indicate that they hold at least one of 12 types of sensitive/confidential company data. Seven out of ten (69%) indicate they hold current financial data, while two-thirds (66%) indicate they hold customer contact details. Other types of data SMBs hold include:

Types of Sensitive and Confidential Company Information SMBs Hold



Though SMBs are most likely to hold current financial data, few indicate that they are actually able to track where this data is stored at any one point in time. SMBs are most successful tracking customer account details and staff salary details.

Types of Sensitive and Confidential Company Information SMBs Hold Versus Tracked



Based on the chart above, SMBs do the best job tracking their customer account details and the worst job tracking their market research/market intelligence data. Overall, it appears that there are a number of areas where sensitive and confidential information could potentially be compromised.

SMBs that use hosted services are not only more likely to categorize company data according to sensitivity and restrict access accordingly, but are also more likely to track sensitive and confidential information.

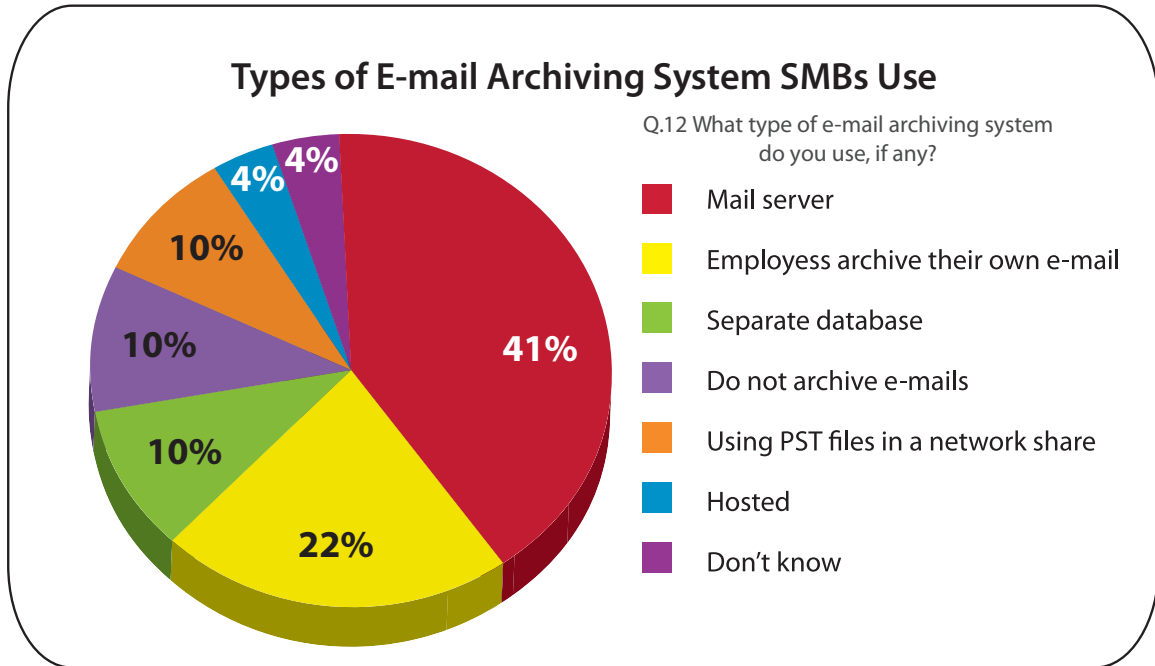
SMBs that are more concerned about internal threats tend to do a better job tracking sensitive and confidential information than the SMBs that are more concerned about external threats.

SMBs with less than 10 employees are the least likely to track any of the various types of sensitive and confidential data. Overall, SMBs with at least 100 employees but less than 250 employees do the best job tracking this type of information. The few exceptions are that the largest SMBs (250-500 employees) do the best job tracking staff employment records, sales prospects databases, and market research/intelligence data.

E-Mail Systems and Archiving

SMBs favor two types of e-mail archiving systems – archiving on internal mail servers and archiving by individual employees. Two-thirds of SMBs archive their employees’ e-mails using one of these two methods.

One in ten (10%) indicates that their company does not archive e-mails, and just 4% archive their e-mails using hosted services.



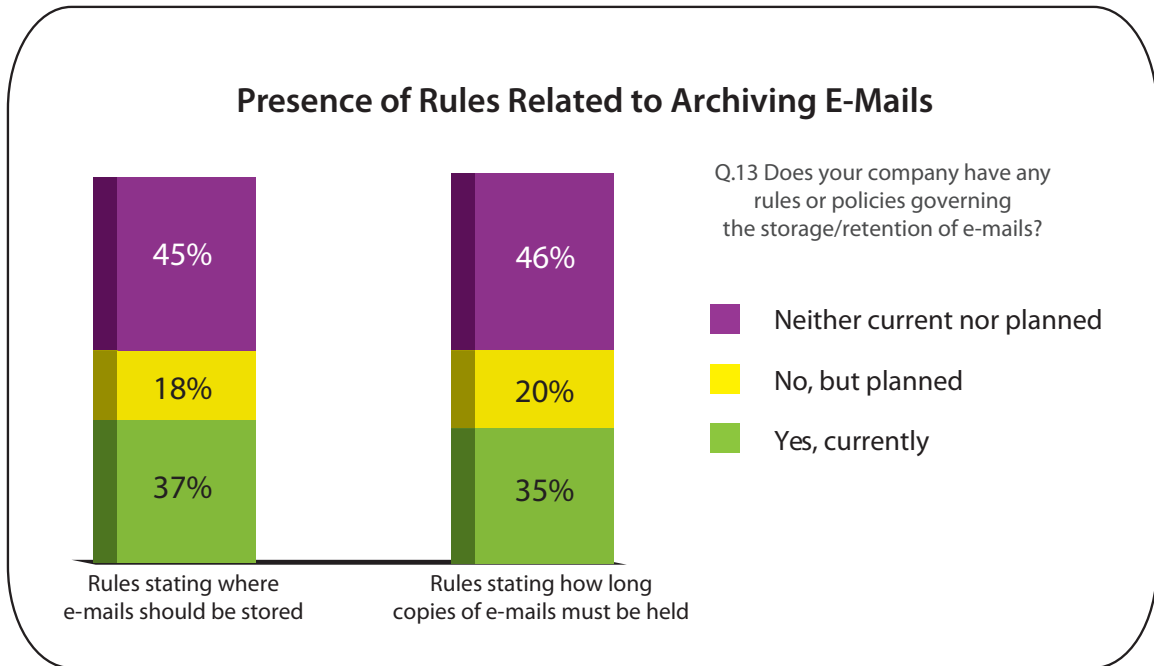
Clear differences in e-mail archiving system preference exist among various sized SMBs. For example:

Table 7
Q.12 What type of e-mail archiving system do you use, if any?

	Number of Employees			
	<10	10-99	100-249	250-500
E-mails are stored in a separate database	7%	7%	13%	23%
We do not archive e-mails	12%	11%	8%	5%

Few SMBs have rules or policies governing e-mail storage or retention.

Slightly more than one-third of SMBs have rules stating where e-mails should be stored (37%) or how long copies of e-mails must be held (35%). However, 18% of SMBs that currently do not have rules stating where e-mails should be stored are planning on creating rules, as are 20% of SMBs that currently do not have rules stating how long copies of e-mails must be held.



Expectedly, larger companies are more likely to have rules and policies stating where e-mails should be stored and for how long.

Table 8
Q.13 Does your company have any rules or policies governing the storage/ retention of e-mails?

(Percent indicating "Yes")	Number of Employees			
	<10	10-99	100-249	250-500
Rules stating where e-mails should be stored	28%	35%	42%	59%
Rules stating how long copies of e-mails must be held	26%	30%	43%	54%

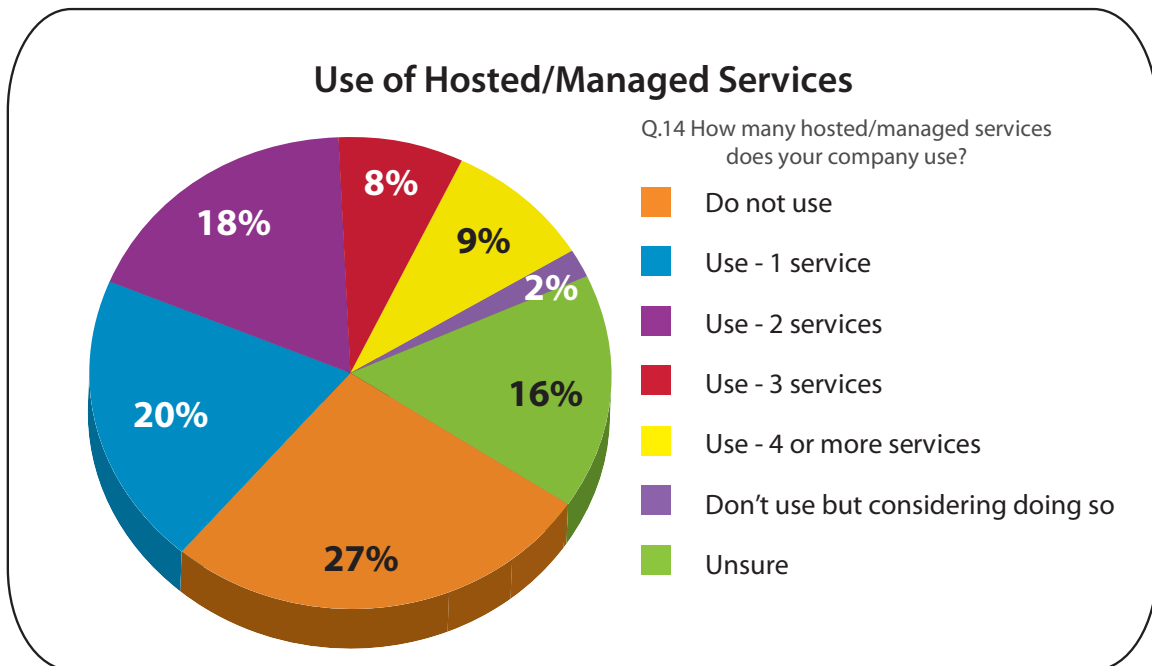
SMBs using hosted services are more likely than SMBs not using hosted services to have rules and policies governing storage and retention of e-mails.

Similarly, SMBs that are more concerned about internal threats, compared to SMBs more concerned about external threats, are more likely to have rules and policies governing storage and retention of e-mails.

Hosted/Managed Services

Twice as many SMBs use hosted/managed services as do not. Among those who use these services, no single set-up dominates.

Fifty-five percent (55%) of SMBs stated that they use one or more hosted/managed services, while 27% indicate they do not use any hosted/managed services. The remainder are either considering (2%) using hosted/managed services or do not know if they use any (16%).



Once a company gets 10 or more employees, the likelihood that the company will use hosted/ managed services increases greatly.

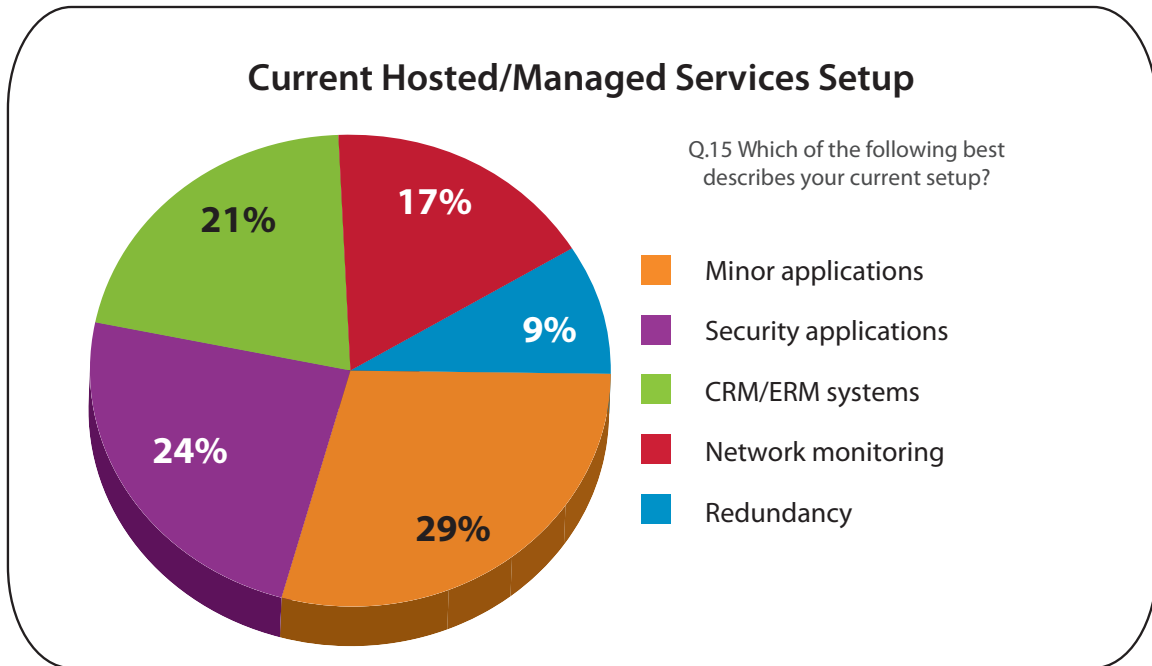
Table 9
Q.14 How many hosted/managed services does your company use?

	Number of Employees			
	<10	10-99	100-249	250-500
Do not use hosted/managed services	41%	19%	18%	17%

Beyond the fact that SMBs with fewer than 10 employees are most likely to use just one hosted/managed service, there is little discernible pattern in use based on company size. For example, large SMBs are not necessarily more likely to use more hosted services.

Hosted/managed services are used by SMBs for multiple reasons, with no single set-up serving as a primary reason for use.

Of the SMBs that use at least one hosted/managed service, 29% state that the services are used for minor applications, 24% are used for security applications, and 21% are used for CRM/ERM systems. The remaining SMBs use the services for network monitoring or for redundancy.



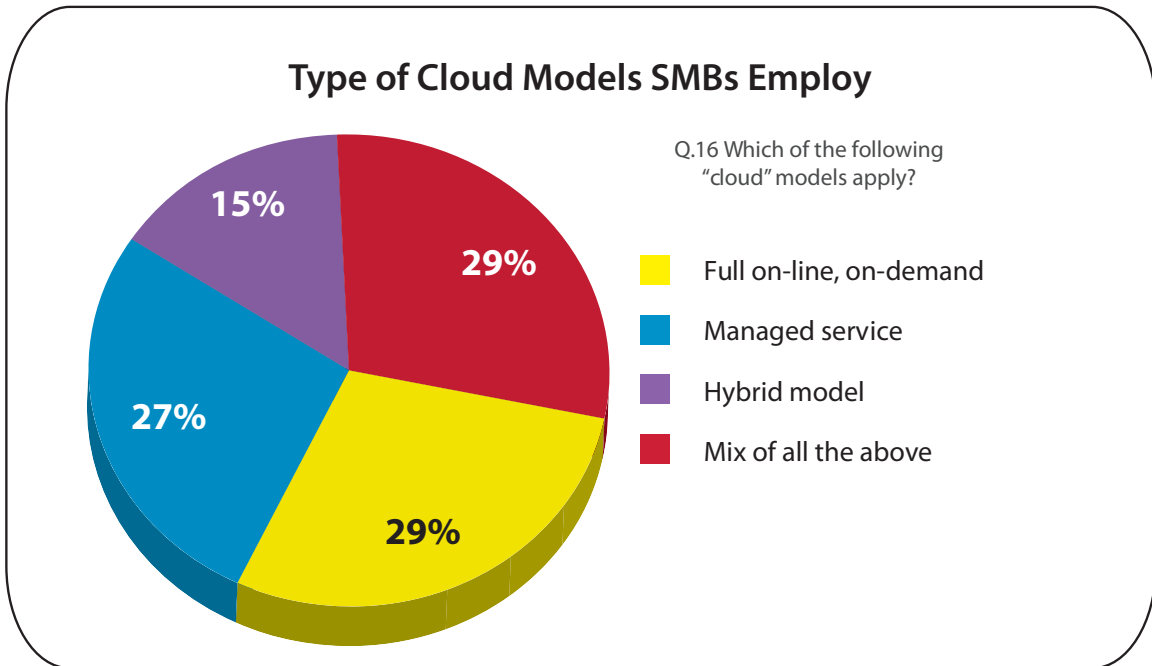
Though no single setup appears to dominate, certain setups are more prevalent based on company size.

Table 10
Q.15 Which of the following best describes your current setup?

Used for....	Number of Employees			
	<10	10-99	100-249	250-500
Minor applications	48%	24%	15%	19%
Security applications	20%	29%	28%	16%
CRM/ERM systems	13%	23%	28%	26%
Network monitoring	13%	13%	24%	21%
Redundancy	6%	11%	4%	19%

Among the cloud models in use today, more SMBs are likely to exploit a full on-line, on-demand model than a managed service or a hybrid model.

Three out of ten (29%) SMBs indicate that the full on-line, on-demand cloud model applies to their situation, which is the same percentage that replied uses a mix of the three models – full on-line, on-demand; managed services; and hybrid model. Further, 27% state they use the managed service model, and 15% use the hybrid model.



SMBs with between 100-249 employees are the most likely to use a hybrid model, while SMBs with less than 10 employees are most likely to use a full on-line, on-demand model.

Table 11
Q.16 Which of the following "cloud" models apply?

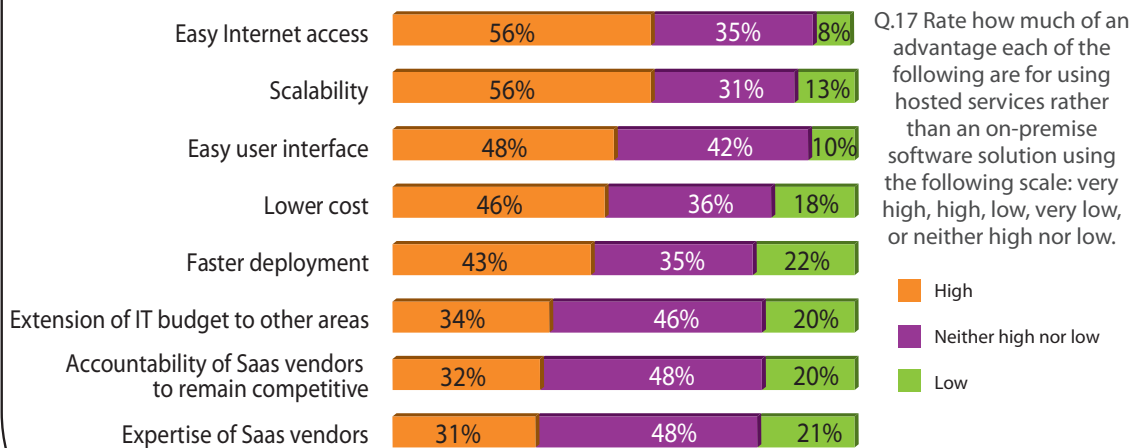
Used for....	Number of Employees			
	<10	10-99	100-249	250-500
Full on-line, on-demand	35%	34%	13%	30%
Managed service	24%	24%	30%	33%
Hybrid model	12%	14%	22%	14%
Mix of all of the above	29%	27%	34%	23%

SMBs that are more concerned with external threats are almost twice as likely as SMBs that are concerned with internal threats to use a mix of all three cloud models (31% vs. 17%, respectively). Perhaps this choice is a reflection of these companies' concerns with external threats.

Easy Internet access and scalability are the top two advantages that SMBs see for using hosted services.

SMBs rated easy Internet access and scalability as the top advantages of using hosted services rather than an on-premise software solution. The advantages associated with SaaS vendors (expertise and accountability) were rated as the least advantageous reasons for using hosted services.

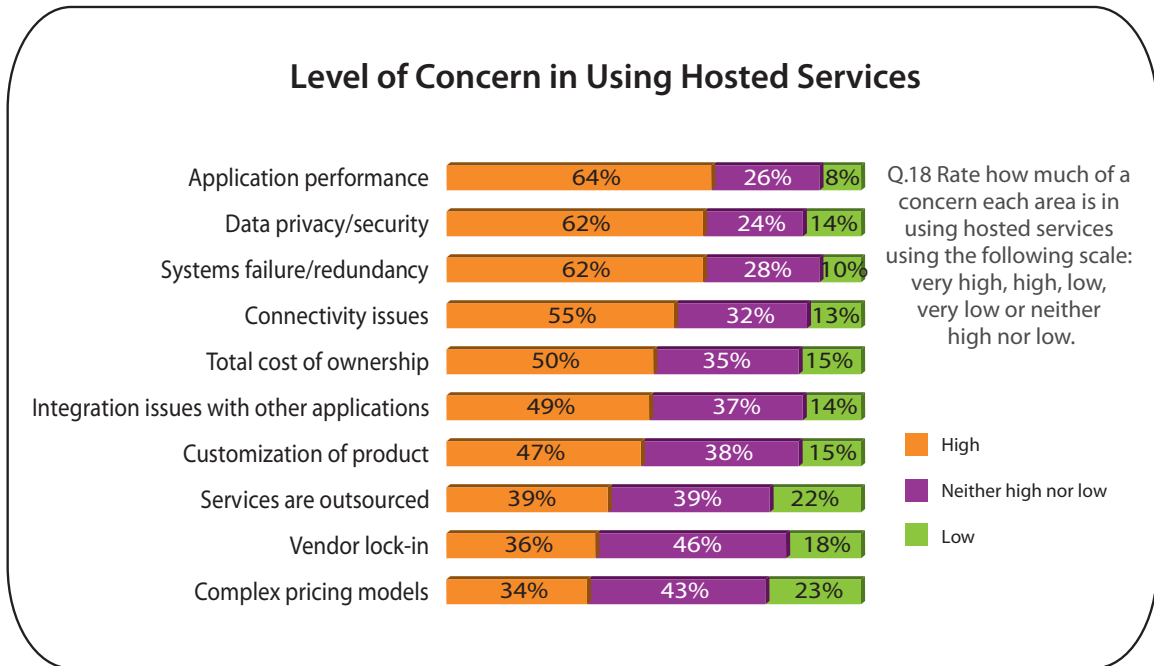
Advantages for Using Hosted Services



There is no discernible pattern in terms of which factors are of greater advantage for one company versus another based on the company size.

Application performance, data privacy, and systems failure are the biggest concerns of SMBs in using hosted services.

Between 62% and 64% of SMBs indicated that application performance, data privacy/security, and systems failure/redundancy are of high or very-high concern when using hosted services. These three areas received the highest concern. On the other end, SMBs are least concerned about vendor lock-in or complex pricing models, where a little over one-third indicated these areas were of high or very-high concern.

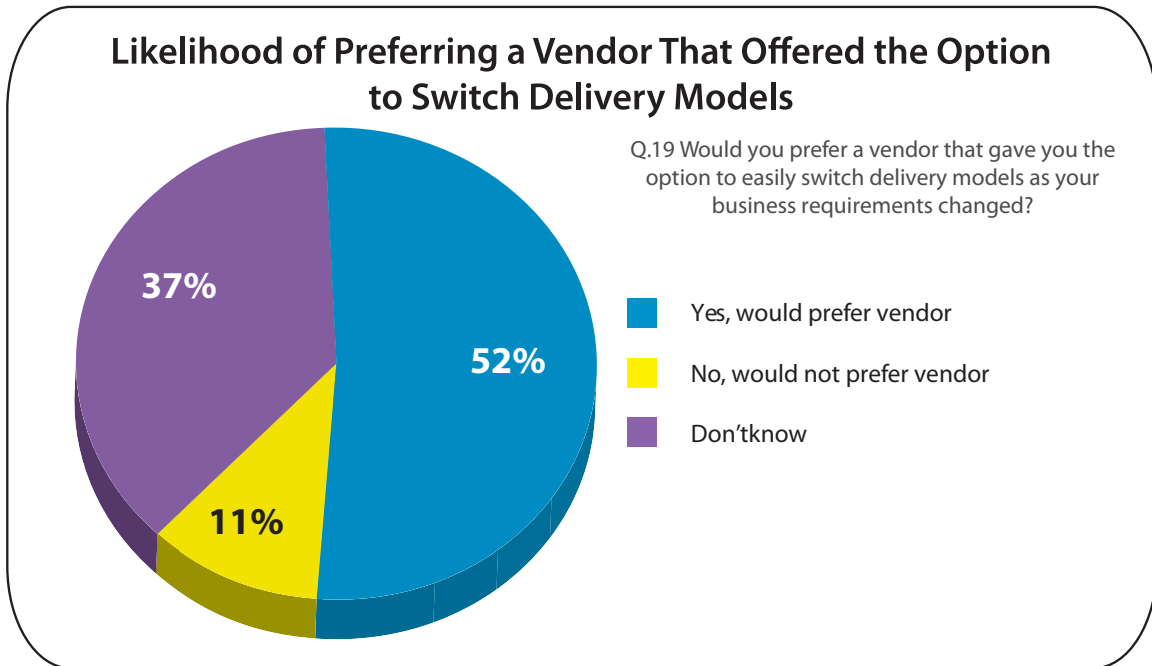


Overall, SMBs with between 250-500 employees tend to be less concerned with the various areas as a result of using hosted services, with the exception of

- » Integration issues with other applications
- » Services being re-outsourced
- » Complex pricing models

More than half of SMBs indicate they would prefer a vendor that gave them the option to easily switch the delivery model as their business requirements changed.

Just over half (52%) of SMBs would prefer a vendor that gave them the option to easily switch models as their business requirements changed, which is almost five times as many who said they would not prefer a vendor who provided that option (11%). Just over one-third (37%) indicated that they were unsure if they would or would not prefer a vendor who provided this option.



Larger SMBs are much more likely to prefer a vendor that allowed the option to switch models.

Table 12 Q.19 Would you prefer a vendor that gave you the option to easily switch delivery models as your business requirements changed?				
	Number of Employees			
	<10	10-99	100-249	250-500
Yes, would prefer vendor	41%	52%	62%	65%

