Driving With the Brakes On

Is your organisation slowed down by information risk concerns?

By Jon Collins, June 2010

In a nutshell:

While much attention around information risk is on medium and large companies, recent research from Freeform Dynamics suggests that smaller organisations are just as susceptible to the risks. Indeed, in some cases organisations feel unconfident about how they take their organisations forward. So, how can such concerns be dealt with? In this report, we look at how management best practice and technology work in tandem to reduce the level of concerns.

Key points:

- Factors such as regulation and use of sensitive data are having an influence on the level of risk experienced by smaller companies. As a result, certain industry segments are more susceptible than others, but they are not all taking their responsibilities seriously.
- The knock-on effect of a lack of security is that smaller organisations do feel held back, for example when it comes to adopting more distributed working practices, or how they share information with suppliers and customers.
- All the same, organisations are not necessarily making appropriate investments in terms of management and technical capabilities. This can result in a vicious circle between inaction on the one side, and feeling held back due to a lack of confidence on the other.
- This is a solvable problem, but it needs to be solved through non-technical means in parallel with technical means.
- We can learn from the experiences of more forward-thinking organisations in terms of what makes a difference, with factors including senior management buy-in, appropriate policy setting and awareness rising across the workforce.

The research upon which this report is based was designed and interpreted on an independent basis by Freeform Dynamics. During the study, which was sponsored by Symantec, feedback was gathered from 700 small businesses (10-100 employees) across EMEA via in-depth telephone interviews.

Research sponsored by

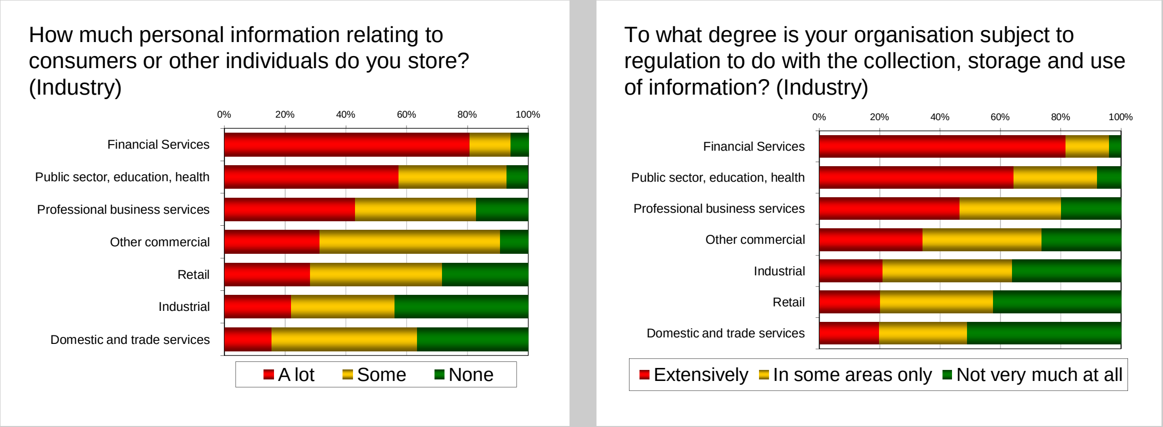
symantec.

Introduction

Security professionals talk a lot about ‘information-related risk’, but just what does that mean in the context of smaller organisations, and does it really impact how business is done? In this research study, conducted during Spring 2010, we wanted to build a picture of how smaller organisations across Europe were sensitive to specific pressures and concerns around information risk, and what, if anything they were doing about the challenges.

To build a picture of such risk levels, we asked interviewees a number of questions around sensitivity to risk, including how dependent smaller organisations were on certain kinds of data, what impact might there be should it fall into the wrong hands, and to what level organisations were subject to regulation around information collection, storage and use, and so on.

Individual answers make interesting reading – not least looking at how the level of regulation varied between sectors. As we can see from Figure 1 for example, organisations operating in the financial services sector are more likely to store information on individuals than other sectors; this adds some perspective on the level of regulation to which such organisations are subjected. As a result, often it may be the industry an organisation operates in that dictates the rationale for security investments, rather than non-industry-specific questions for example around the cost of a breach.



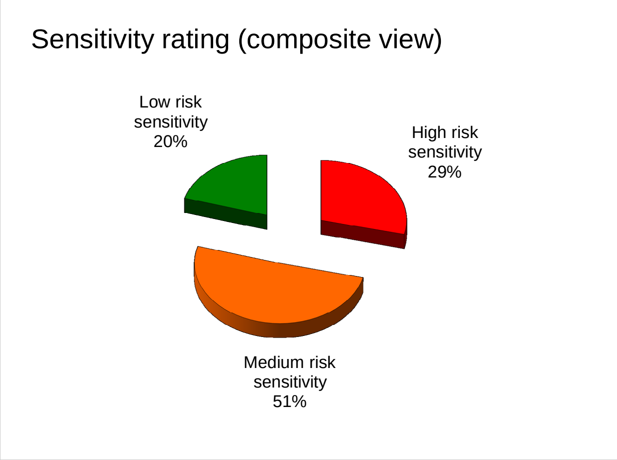
How much personal information relating to consumers or other individuals do you store? (Industry)

To what degree is your organisation subject to regulation to do with the collection, storage and use of information? (Industry)

There are some interesting differences by industry, notably that financial services organisations are more affected than other verticals.

Figure 1

We can see quite clearly from the responses that smaller companies are subject to similar pressures as larger organisations, a factor that is sometimes overlooked. What’s interesting is whether corporate behaviour varies depending on such factors. To determine what steps organisations are taking, and whether they make any difference to their sensitivity to risk, we first built a composite ‘sensitivity rating’ from the responses (Figure 2). We shall be using such composite views to determine what best practices and technical measures make a difference.

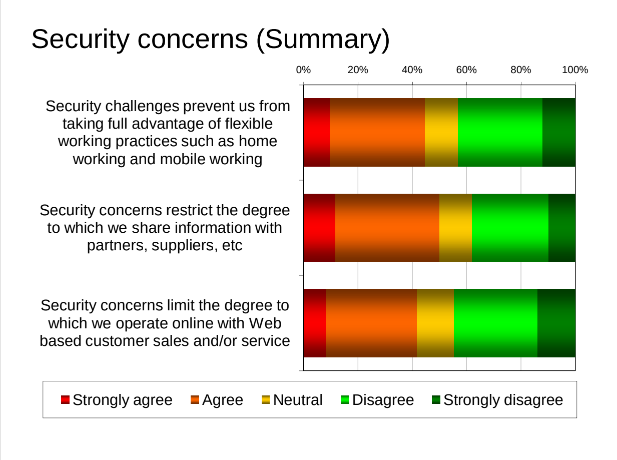


The sensitivity rating contains a composite view of criteria such as use of sensitive data, level of regulation and potential impact should a breach occur.

Figure 2

Are organisations held back by security concerns?

Before we drill into solutions however, let’s first consider whether there is a problem to be solved. When we asked questions around whether security concerns were holding organisations back, we found that over 40% of respondents felt in some way constrained by fears around specific risks (Figure 3).

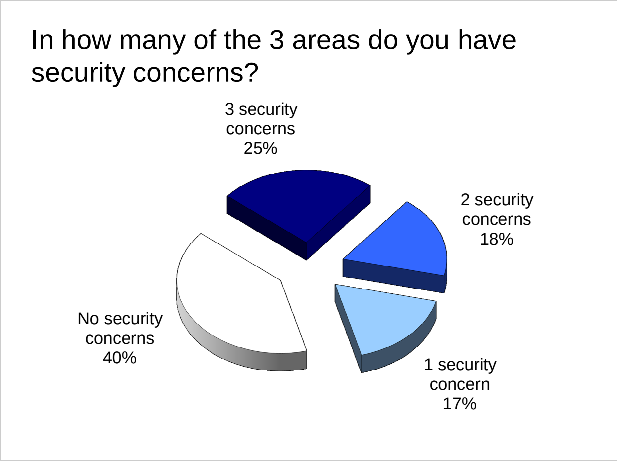


Over 40% of respondents have concerns in each area cited.

Figure 3

In other words, many organisations see the perceived lack of security as a significant challenge. The implication is that a lack of security is actually getting in the way of the organisations growing their businesses in directions they’d like to take them: absence of confidence is in the best case slowing things down, and in the worst case, preventing them from happening altogether.

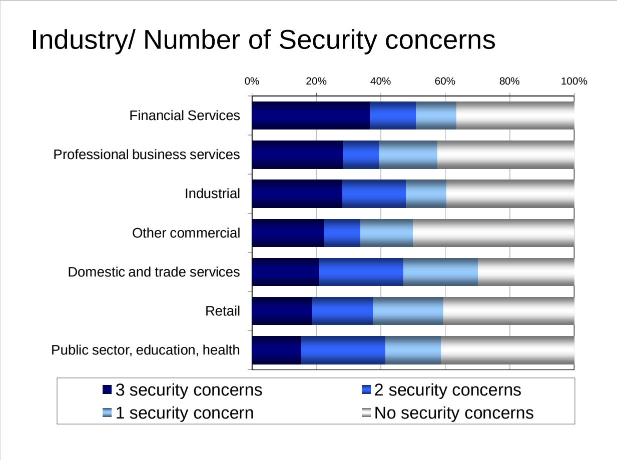
This picture becomes even more stark if we rank respondents according to the number of concerns. As can be seen from Figure 4, 59% of respondents had concerns in at least one area, and a quarter felt that all three areas were of concern. Interestingly, 40% say they have no such concerns – this does beg the question of whether they are deluding themselves!



60% have security concerns in one or more areas.

Figure 4

While there is clearly an issue however, we should not panic about overall levels of concern: all organisations will be different and some concerns will be for perfectly valid reasons. If we look again at the financial services sector for example – and remembering that this sector is responsible for larger amounts of sensitive customer data, and is subject to sometimes onerous regulation as a result – it should come as no surprise that security concerns in this sector are seen as greater (Figure 5).



More organisations in the financial services sector feel held back by security concerns than in other sectors.

Figure 5

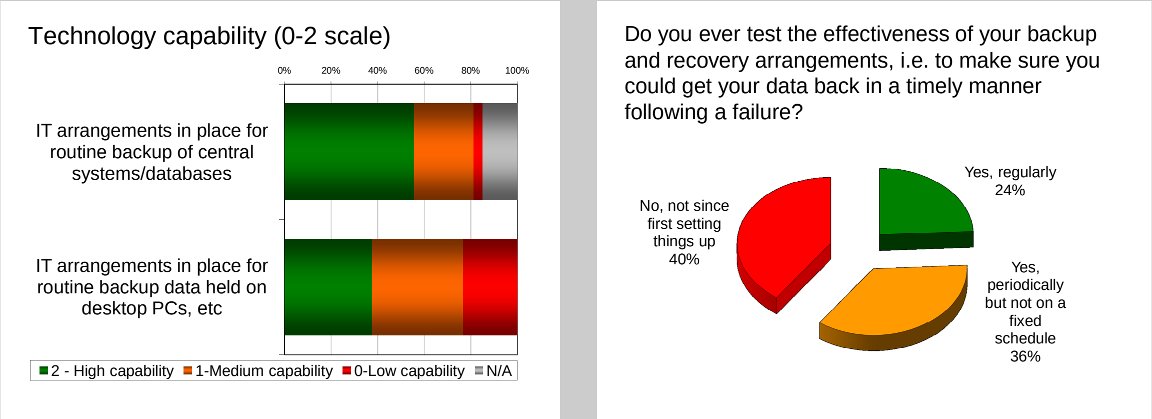
This doesn't let all organisations off the hook of course. If we compare this figure with Figure 1 for example, we can see how public sector organisations are also highly regulated, and dealing with large quantities of customer data, and yet they do not have the same security concerns – suggesting a level of complacency, if not negligence.

What is clearly obvious is that smaller businesses across Europe feel they are unable to progress due to fears about security in these, and no doubt in other areas. In other words, from a business perspective this amounts to opportunities being missed and business growth being slower than it could perhaps be. This is partially down to organisations not having their own houses in order, which we look at next.

Taking off the rose tinted spectacles

The traditional view on security in general and IT security in particular is that it is about protecting the periphery of the organisation from the ‘bad guys’, the hackers and cybercriminals. As a knock on effect, this can play to the human trait of assuming that “Bad things only ever happen to other people.” As the data we shall look at suggests, we can lull ourselves into a false sense of security about the threats, adopting an ignorance-is-bliss approach even while feeling uneasy about the consequences.

To illustrate some of these points, we will look at some of the specific responses in the study. For example, let’s consider smaller business attitudes to backup and recovery. As shown in Figure 6, clearly many organisations feel they are doing backups, particularly for centralised systems. That’s a good thing, right?

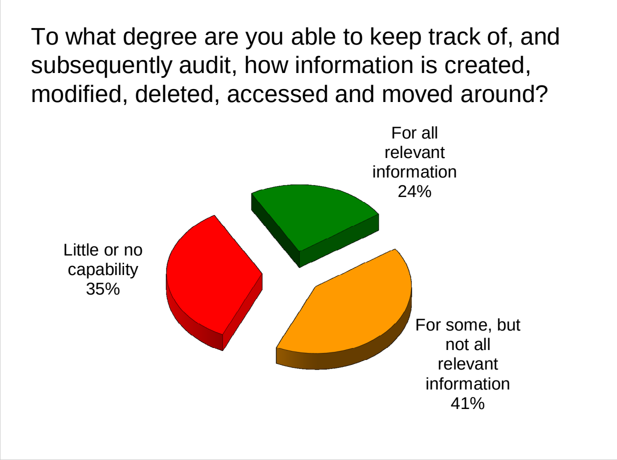


Backups may be happening, but testing of restoration from backups is not.

Figure 6

However, we know from experience that backups are only one part of the story, and that organisations have found themselves in difficulties when it comes to restore time, because the backups don’t necessarily work. It is only by testing backups that you can really be confident that you have protected yourself against information loss or damage. According to the respondents, only a quarter are testing their backups on a regular basis, which means that the remaining three quarters are leaving themselves to some extent exposed.

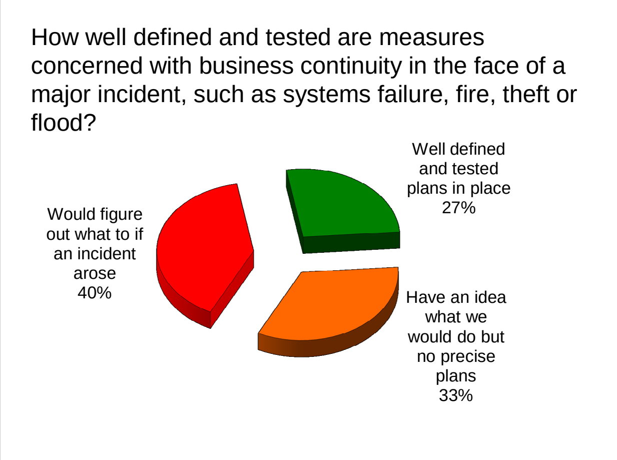
A second example of how organisations could be doing a better job when it comes to information risk management can be seen in terms of keeping track of information assets. In layman’s terms, if you don’t know what information you have and who can access it, it becomes harder to secure and protect the information. As can be seen from Figure 7, only a quarter of organisations profess to being able to keep track of all relevant information.



Only 24% of respondents are able to keep track of their information assets.

Figure 7

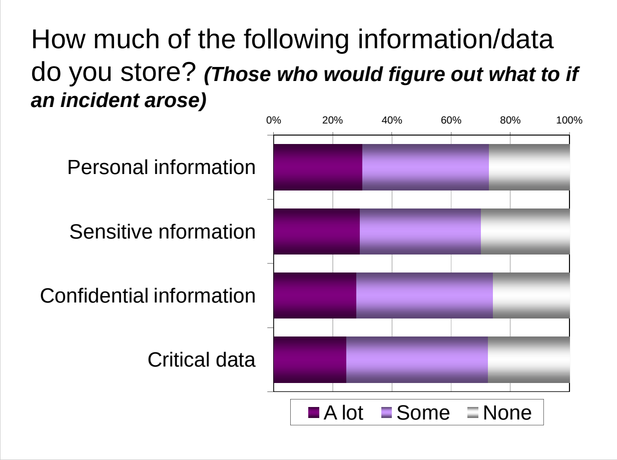
For a third and final example, we can look at business continuity – what measures are in place if something untoward were to happen? As can be seen from Figure 8, only 27% of respondent organisations have a well defined and tested business continuity plan in place. Perhaps the most significant figure here is that almost 40% would just figure out what to do should an incident arise, which on the surface is quite an indictment.



40% of the sample are reliant on coping strategies when it comes to business continuity.

Figure 8

Perhaps, goes the argument, those organisations who would ‘cope’ are not those storing significant quantities of information? A closer look reveals the types of information stored with this group of companies – as you can see, there are still significant quantities of sensitive information involved (Figure 9).



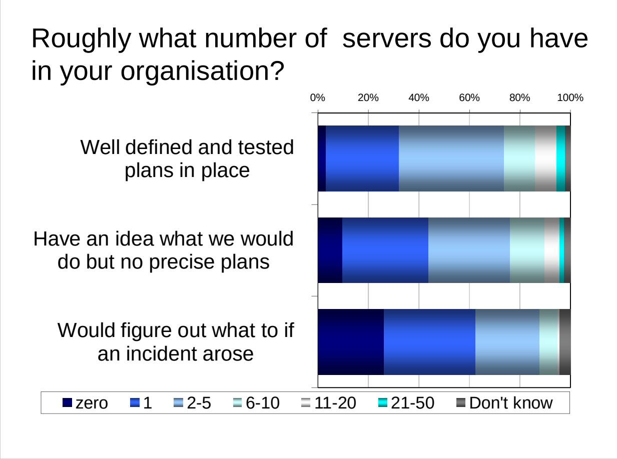
Information stored by organisations which profess no more than 'coping strategies' in the face of a major incident.

Figure 9

To make it clear, here is how we defined each bar on the chart above:

- **Personal Information**: Relating to consumers or other individuals.
- **Sensitive information**: That would be financially, legally or otherwise damaging should it fall into the wrong hands.
- **Confidential information**: Relating to other businesses you trade with, e.g. suppliers, customers, partners.
- **Critical data**: Would cause some parts of the business operation to stop if it were not available.

While it is clearly the case that some smaller organisations in Europe are not taking their information management responsibilities seriously, we should recognise that this is a complex area. Numerous criteria are going to influence the level of planning in place, not least for example the amount of IT equipment in place (and therefore perhaps, whether there is a defined responsibility for managing it). For example, Figure 10 shows that the proportion of 'coping' organisations falls quickly relative to the number of servers in place.



The amount of planning taking place increases proportionally to the number of servers in place.

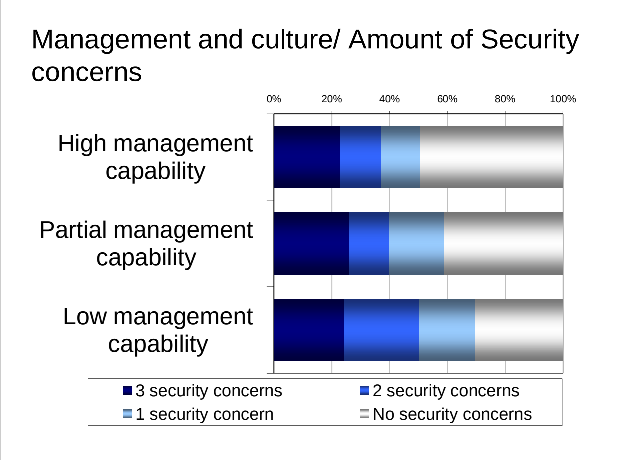
Figure 10

This is not to let those without any servers in place off the hook, of course. Even if you are a three-person company reliant only on laptops, you should perhaps still consider what kinds of things might go wrong, and what you would do about them. However, this is indicative of a wider point: that when it comes to solving the challenges, there is not going to be a one-size-fits-all answer. Let's take a look at the options.

Dealing with concerns around security and information risk

To summarise so far: the direct consequence of information risk concerns is that businesses feel held back, but such organisations are not necessarily doing themselves any favours when it comes to putting the basics in place. Of course organisations will be reticent to put time, effort and indeed money in place if there is no guarantee of return. So from a business standpoint the question becomes, “Would making any effort in these areas really make a difference?”

We can get a clear answer to this question when we look at composite views of responses across both management capabilities in place, and the technical mechanisms used to enable, support and automate them. When we looked at the overall management and culture capability of the respondents, it was quite obvious that those with low management capability had more concerns around information risk and security than those with a higher level of management capability in place (Figure 11).



A high management and culture capability reduces the number of concerns. Low capability increases the concerns.

Figure 11

Specifically, companies where senior management and/or IT leadership are highly tuned in to issues associated with information access/security and information management/protection fare a lot better than the organisations where management are not aware. For example, such companies are more likely to have up to date security policies that are proactively monitored; they also tend to have well defined and tested plans in place concerned with business continuity in the face of a major incident.

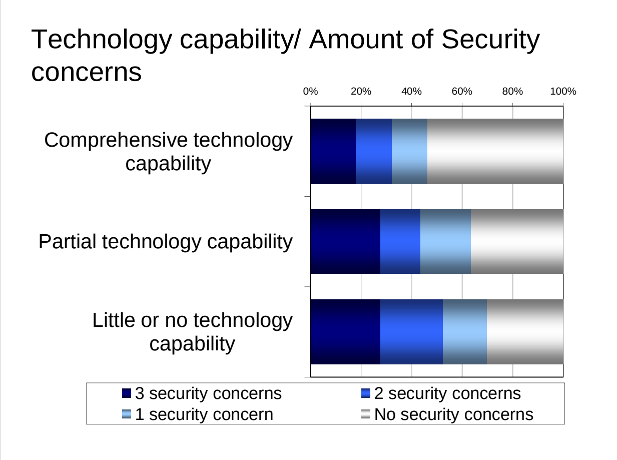
These organisations are also more likely to consider factors that might impact information security and protection during recruitment, (e.g. awareness of risks, responsible attitude, etc) and to train staff on matters of information security, (e.g. protecting access rights, responsible document distribution, use of external email, social networks, etc) and on matters of information protection (e.g. backup discipline, prevention of data loss and corruption, etc).

It is plain to see why such considerations go a long way to reducing the number of security and other risk-related concerns. The message is not just that better-managed organisations have fewer concerns than less-well managed organisations, however. Rather it indicates a stark choice: if smaller organisations across Europe want to be able to move their businesses forward in the face of such concerns, they need to get their own houses in order.

Incorporating the role of technology

Not only do management and culture capability affect the number of security concerns, technology capability also plays a part. Again, technology can be used in a number of ways, for example in terms of end point protection, backup, recovery and archiving, systems monitoring and management, and so on. What we are most interested in, is the composite view considering how well such capabilities are being embraced as a whole.

As shown in Figure 12, there is once again a correlation between capability (in this case technology capability) and a reduction in the number of security concerns. In other words, organisations that have implemented the right mix of technologies do feel more confident than those who have not.

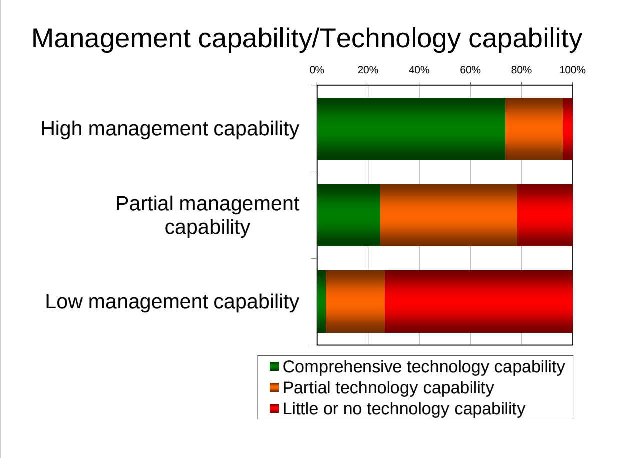


Technology has an important part to play in reducing concerns.

Figure 12

It's interesting to note from the chart that "partial technology capability" does not appear to have that much of an effect on the level of security concerns addressed. Clearly, there is a threshold to be crossed in terms of capability – there is no point tinkering around the edges.

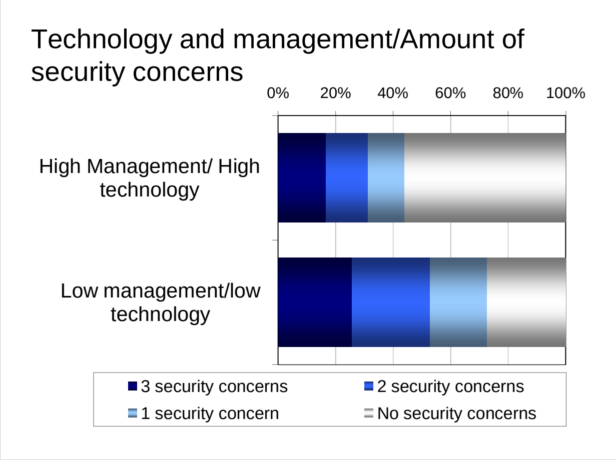
So which is more important – getting the management right, or getting appropriate technologies in place? There is no direct answer to this question as they go hand in hand. As shown in Figure 13, there is a very strong correlation between the two – organisations with a high level of management capability are far more likely to have a comprehensive technology capability in place.



Those who have the right technology in place are those companies who have a high management and culture capability

Figure 13

Given how management and technology go hand in hand, what is their combined impact on security confidence? Figure 14 shows just how much difference it makes to the number of perceived concerns, and hence to the ability to move a business forward. Overall, organisations with comprehensive measures in place are twice as likely to have no security concerns at all – which is quite a result.



A combination of culture and management capability and technology capability drastically reduces the amount of security concerns.

Figure 14

This fits with common sense but it is good to see it in black and white terms. Arguably, you cannot have comprehensive security without good management – as what you cannot manage, you cannot secure.

Conclusion

While we sometimes talk about security being a business enabler, it is quite clear that a concern around a lack of security is holding back smaller organisations across Europe. The irony of course, is that the general lack of will to do anything about security risks is resulting in organisations that feel held back in the first place.

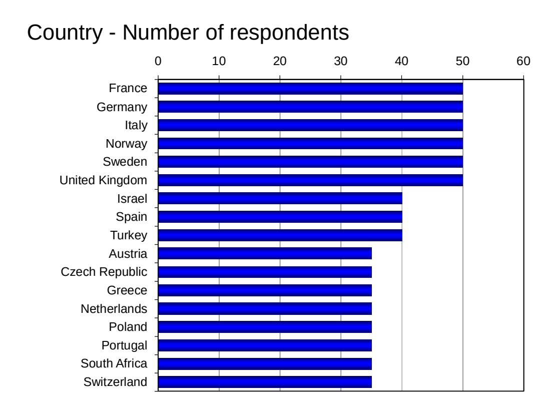
The advice is clear: this is a deadlock every organisation can break for itself, by seizing the nettle and determining what it needs to do to address its own security concerns. Given that we are talking about the smallest organisations here, this does not have to be an onerous exercise at all: indeed, the effort required could probably be measured in hours, rather than weeks.

This is not a negative finding, indeed there is a very positive reason to take a proactive approach to security, but it does require appropriate effort. Organisations that want to get their houses in order can move forward in confidence and derive the business benefits that can result from operating a more front-foot operation. Doing nothing is still an option, but in the recognition that the business is harming nobody's prospects but its own.

Appendix A

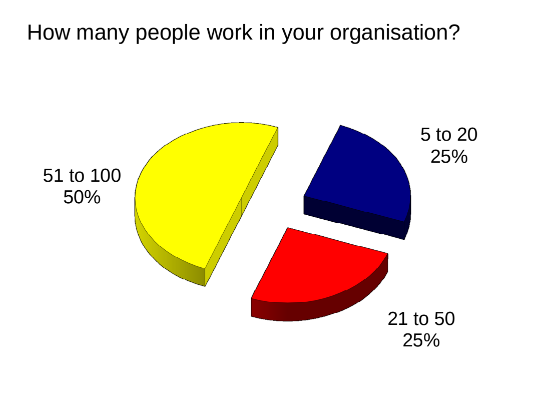
Research Sample

The study from which these inside tracks have been produced was designed and executed by Freeform Dynamics in Q1 of 2010, via a telephone survey of 700 small businesses in Europe.



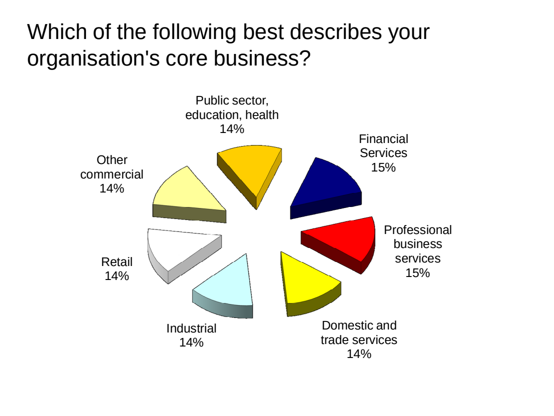
The research sample explored the experiences and capabilities of 700 small businesses across 17 countries in EMEA

Figure 15



The sample was targeted at the 'small' end of the SMB sector

Figure 16



A balanced sample was taken from a range of industries

Figure 17

About Freeform Dynamics

Freeform Dynamics is a research and analysis firm. We track and report on the business impact of developments in the IT and communications sectors.

As part of this, we use an innovative research methodology to gather feedback directly from those involved in IT strategy, planning, procurement and implementation. Our output is therefore grounded in real-world practicality for use by mainstream business and IT professionals.

For further information or to subscribe to the Freeform Dynamics free research service, please visit www.freeformdynamics.com or contact us via info@freeformdynamics.com.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organisations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

More information is available at www.symantec.com.

Terms of Use

This document is provided for your general information and use only. Neither Freeform Dynamics Ltd nor any third parties provide any warranty or guarantee as to the suitability of the information provided within it for any particular purpose.