The Impact of IT Security Attitudes

Putting the pieces in place for effective security delivery

Jon Collins, Freeform Dynamics Ltd, September 2008

Much has been written about the existence of various threats, internal and external, and vendors are only too quick to proffer solutions to the problems. But what really needs to exist for security to work? This report considers some of the more behavioural aspects of security best practice, such as the role of awareness, policy and communications.

KEY FINDINGS

IT security matters - but some organisations are doing better than others

While IT security is generally seen as important to our IT-oriented research sample, there is a general feeling that such aspects as the level of security awareness, and how seriously IT security is taken by business management, could be better. Such characteristics can be used to determine organisations that generally are ahead of the pack, and those who are lagging behind.

Leading organisations believe themselves to be better protected, and rightly so

In general, organisations that we have categorised as 'leaders' believe themselves to be better protected than the 'laggards'. It is not always as simple as this when it comes to a reduction in threat levels, as it will tend to be those threats that are directly influenced by good security practices, that show the most marked improvements.

Having a comprehensive security policy is fundamental to good security practice

Organisations with a fully comprehensive, dynamic security policy are less likely to suffer security breaches such as web site defacement, or indeed theft. It is therefore no surprise to note that the more leading organisations are twice as likely to have such a policy in place than the sample as a whole. Equally notable is that organisations with outdated policies fare less well than those with no policy in place at all.

Communication between the business and IT is also important

Few would doubt that business risks should be prioritised as an input to implementing good security practice. There is a big difference of opinion between the leaders and the laggards however, concerning how important it is to communicate this information both to IT, and to the workforce. And indeed, such co-ordination has a tangible impact on risk reduction.

More progressive IT security organisations are deploying more complex tooling

IT security tools are in general bought more on the basis of simplicity than need - tools that are easy to cost-justify and deploy are far more likely to be in place than more complex tools. However, leading edge organisations are installing the more challenging tools. The lesson is not to install everything, but to review one's own situation and make the necessary improvements that become apparent.

The research upon which this report is based was designed and interpreted on an independent basis by Freeform Dynamics. Feedback was gathered from 1,102 IT and business professionals during the online study, which was conducted in partnership with The Register.

Introduction

One of the issues with reading about IT security is an overwhelming feeling of, "Haven't we heard it all before?" There is always plenty that can go wrong, and everybody loves a good story about a high-profile failure, a fact only too clear to the vendors of certain security products. It's somewhat troubling that both individuals and organisations are far more likely to spend on security in the period following a major incident: no doubt there are some deep-seated psychological reasons why in general, humans fail to deal with the risks or their consequences in advance (like with driving, where "accidents always happen to someone else.") The perhaps unsurprising, if a little unsavoury, result is that security vendors and their representatives should choose to maximise the publicity around bad happenings.

As an additional consequence, it can be quite difficult to separate the wood from the trees, the hype from the reality. The average IT manager (if indeed there is such a thing) has to determine which of the wide variety of security products actually is worth apportioning some of his or her limited budget, and there are few security products that do not require some change to how IT is managed. At the easier end of the deployment scale are such products as antivirus and firewall – these share characteristics including:

- The threats they respond to (viruses and hackers, for example) are well understood by both business and IT.
- The terminology is also pretty familiar to most parts of the organisation.
- They are relatively straightforward to deploy, impacting only specific areas of the infrastructure.

At the other end of the scale we have such products as security event management and behavioural analysis software, which do not correspond to such characteristics. Is it any wonder (Figure 1) that we see them right at the other end of the scale.

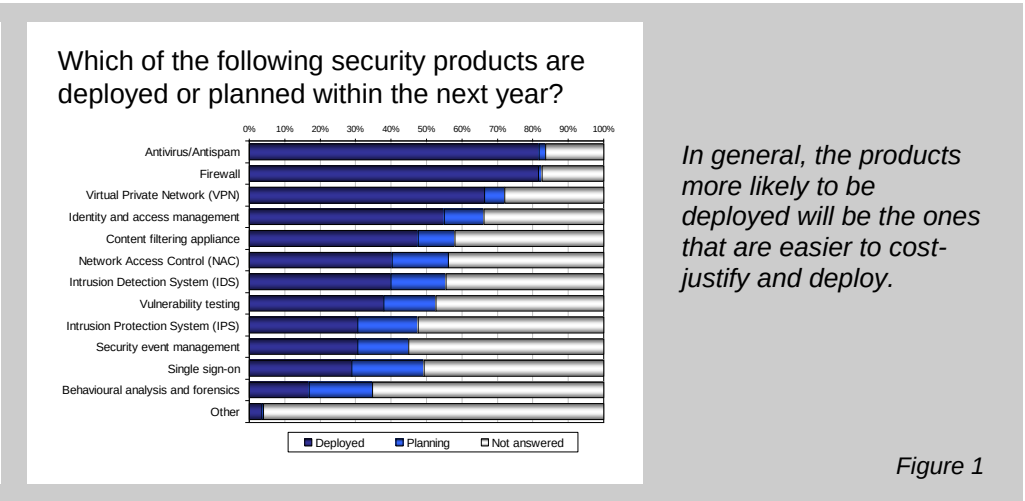


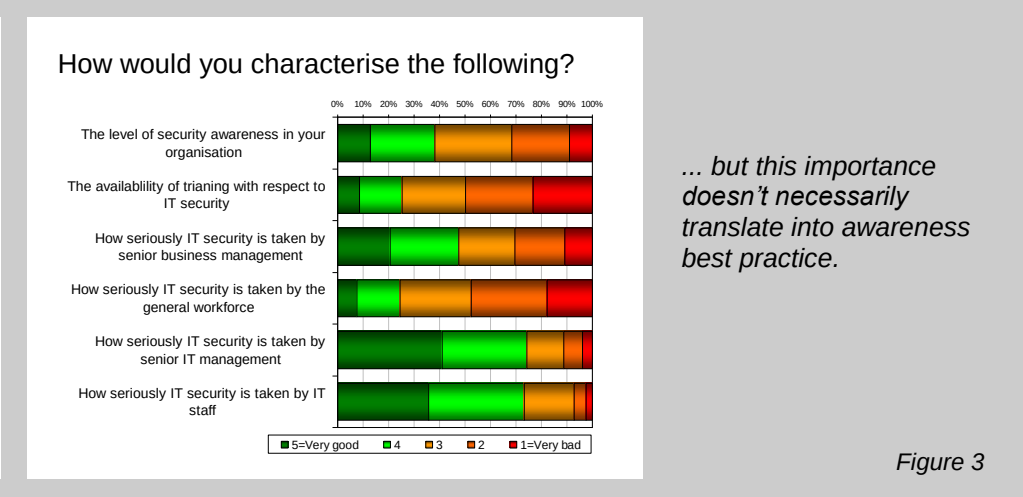
Figure 1

In this study we wanted to cut through the hype and determine what kinds of things determine exactly what does make a difference to the levels of risk organisations face. The study involved in-depth interviews with 1,102 IT professionals. For further information on the research sample please refer to Appendix A.

Does IT security matter?

IT security does indeed matter to organisations across the globe – and indeed it's unlikely anybody would say it didn't matter at all. As shown in Figure 1, externally facing aspects of the business tend to be considered as being roughly equally important, with internal-only areas – product development and staffing – seen as less of a concern.

While there may be general agreement about the principle however, Figure 3 shows that practice in terms of IT security awareness can be variable. Given that the respondents were largely IT staff and management, it is unsurprising perhaps that they should award themselves higher marks. All the same, the results are a bit of an indictment – only a quarter of respondents indicate that IT security is taken seriously by the general workforce in their organisations, for example.



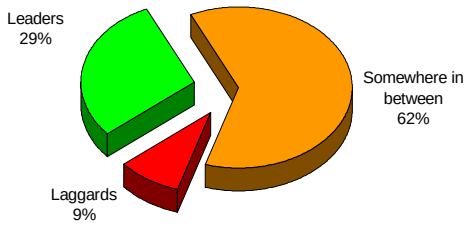
Given the nature of the respondent base, it would be unwise to make any absolute statements about whether businesses 'get' IT security, or otherwise. What we can do however is use the responses to Figure 3 to define a number of groups, which we can then compare to the rest of the data. In Figure 4 we consider the following groups:

- The 'leaders', who answered 4 or 5 to the above questions – 29% of the sample fit in this category
- The 'laggards', who answered only 1 or 2 - this makes up 9% of the sample

Clearly there is no hard and fast rule as to what characteristics are more demonstrative of IT security leadership than others, but equally clearly, it stands to reason that those who can check the

majority of boxes should, in principle, be better off than the others – it is this principle that we wish to test. The majority of respondents lie somewhere in between, but we are most interested in comparing the leaders with the laggards (Figure 4).

A look at the leaders and laggards

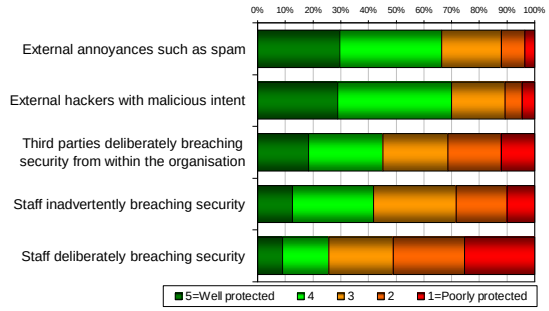


We can separate those who are leading the pack in terms of awareness, from those who are following.

Figure 4

So, does it matter if an organisation is a leader or a laggard? Let us first consider how well organisations think they are protected against IT security threats. From the sample as a whole, we can see that while over two thirds feel they are in some way protected against the 'simpler' threats (as discussed before), far fewer feel they are covered when it comes to more targeted attacks (Figure 5).

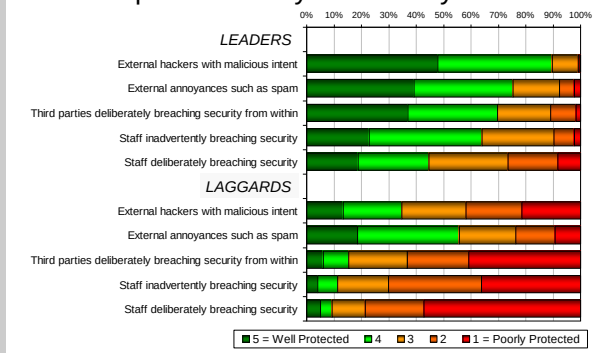
Given everything that you have implemented, how well protected do you believe you are against the following?



The general picture is that simpler threats tend to have been dealt with.

Figure 5

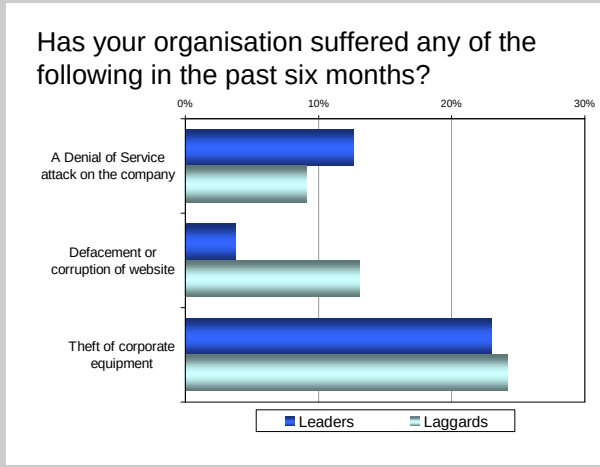
Things get very interesting when we compare the leaders against the laggards with respect to this question. Figure 6 shows our group of leaders feeling they are far better protected across the board, than the laggards.



However, more security-aware organisations consider themselves much better protected than their peers.

Figure 6

But are these so-called leaders deluding themselves? We don't think so. Figure 7 shows how IT security awareness makes little difference when it comes to theft of corporate equipment or denial of service attacks. This is fair enough given that both are largely down to the behaviour of third parties. Where we see a marked difference is where web sites have been defaced or corrupted – in this case, the laggards are three times as likely to suffer than the leaders. In the web site situation, while the problem may be instigated by external hackers, it is up to internal staff to make sure the web site is created in such a way that the risks are minimised.



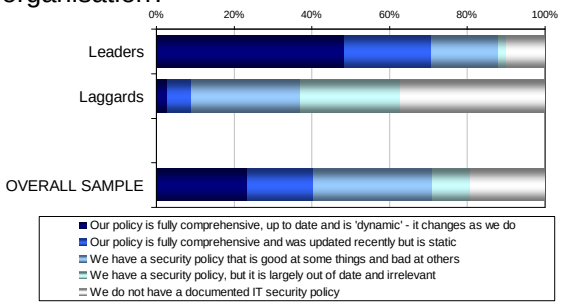
Where threats are more complex, we see a marked difference in likelihood between the leaders and the laggards.

Figure 7

So, while there is clearly not a single answer, we can see that the leaders in terms of IT security awareness are indeed better protected than the laggards. Having reviewed the research findings from this perspective, we have drawn out a number of additional 'good behaviours' around policy, communications and tooling, we look at these now.

The role of policy in delivering IT Security

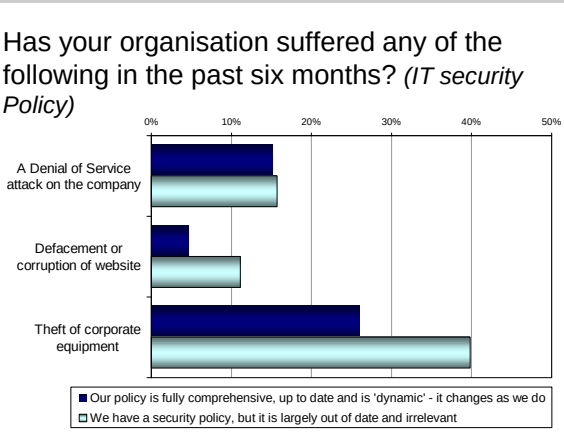
One area that the divide between leaders and laggards was very clear, was in the adoption of security policy. In the sample overall, policy adoption is all over the map – but our 'leader' group were twice as likely to have a fully comprehensive policy in place, as the overall sample (Figure 8). Only a tiny proportion of the 'laggard' group could say the same.



Leading organisations are far more likely to have a comprehensive IT security policy.

Figure 8

The big question in this instance concerns whether the presence of such a policy makes any difference in terms of security issues (Figure 9). As with Figure 7 before, we can see there is little variation in terms of denial-of-service attacks. However there is a marked reduction in the number of incidences of Web site defacement – as well as, incidentally, theft of corporate equipment.

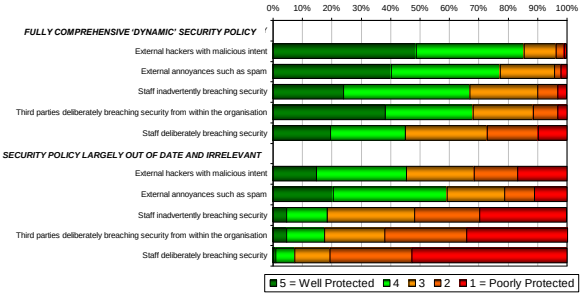


Similarly, having a policy in place has appositive impact on threats such as web site defacement .

Figure 9

We can also see the positive impact of a fully comprehensive IT security policy, on perceptions of protection (Figure 10). This is more than an interesting, yet intangible statistic. We know from previous studies [1] that organisations are often held back from taking advantage of new business practices or adopting new technologies, because of their security concerns. The implication is that more leading edge organisations, with a more positive attitude to security policy, will also be more confident about innovation.

Given everything that you have implemented, how well protected do you believe you are against the following?



Organisations with a comprehensive policy in place feel themselves to be better off, and are likely to be more innovative as a result.

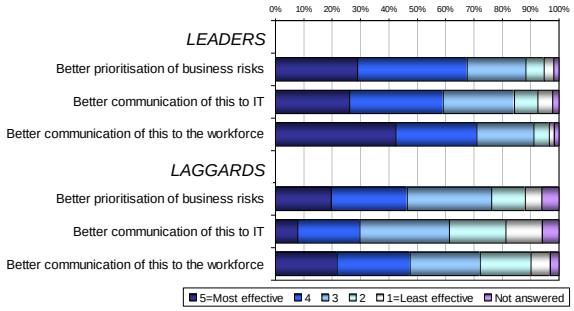
Figure 10

Interestingly, while this is not shown here, having no policy at all is in many cases better than having an old, out of date policy.

Getting the message across

Another area that we can see a significant difference is in terms of communications. As can be seen from Figure 11, there is less of a difference between the leaders and laggards when considering the importance of prioritising business risks. The more marked difference is in terms of how these risks are communicated to the IT department, and to the workforce as a whole.

What do you feel could have the most impact when it comes to improving IT security in general?

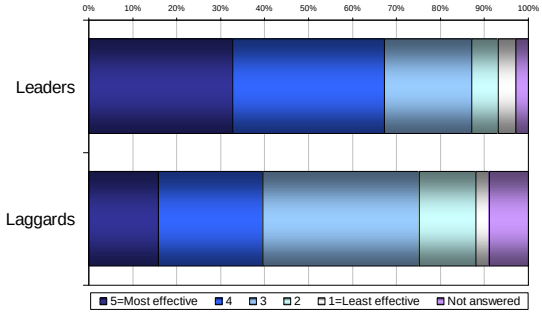


Understanding business risk is important, but more so is communicating risk to IT and the business.

Figure 11

Once again, we need to remember that the respondents to this study are generally in the front lines and management of IT. Considering the above in this context, respondents are saying, “please do tell us what you think the risks are, and more importantly, ensure that business users are fully aware of the risks as well. IT is not washing its hands of the problem however: Figure 12 shows us that it is just as important for IT to be communicating with the business, as vice versa.

What do you feel could have the most impact in IT – better communication with the business?

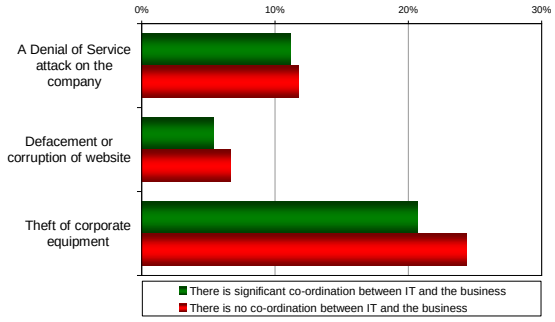


This can be helped with two-way communications between It and the business.

Figure 12

On this latter point, we can also see that it does make a difference by itself – though it is likely that all forms of communication need to be working in tandem in order to have the biggest impact.

Has your organisation suffered any of the following in the past six months? *(IT/Business co-ordination)*

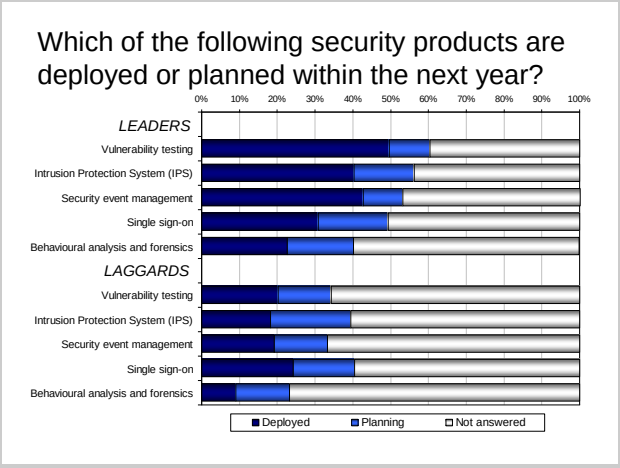


It will be a combination of communications factors that have the biggest effect on risk.

Figure 13

Where do tools fit in?

Good attitudes or policies will not alone protect against the bad guys, of course. Referring back to the initial question of where the 'more challenging' IT security products should fit in, we can gain a clear sign from the leaders category, who are more likely to have deployed such tools (Figure 14) – note that the figure takes the bottom five technologies presented on Figure 1.



Leading organisations are more likely to deploy more complex security technologies.

Figure 14

It is worth mentioning the thorny area of 'planning'. Over a number of research studies, we have learned that while organisations may be considering certain things in their plans, they are not necessarily going to implement them in the stated time period. This is perfectly normal, and is largely down to factors such as changing priorities and unexpected demands. All the same, in the chart above, a far more telling statistic concerns which products have actually been deployed: in all cases, a significantly higher proportion of respondents have adopted such technologies in the leaders category, than in the laggards category.

Discussion and Conclusion

IT security is a complex business, as we have already said, and it can be difficult to unpick the causes from the effects. Is it, for example, that organisations with comprehensive security policies are therefore more security aware, or is it that more security aware organisations are more likely to adopt comprehensive security policies? Or indeed, are their other factors not discussed here, such as whether the information being worked on is particularly sensitive – and is it such factors that dictate both attitudes and the presence of policy?

Such questions are worthy of debate, but they do not change the conclusion that certain behaviours relative to IT security do result in a reduction of both the perceived risk and the actual likelihood of breach. Such behaviours can also be linked to more general best practice in IT, and the beneficial effects, as we have documented in other reports [2]. (One such example, not explicitly documented here, was the highly measurable, positive effect of security best practice on the more general question of IT systems failure.)

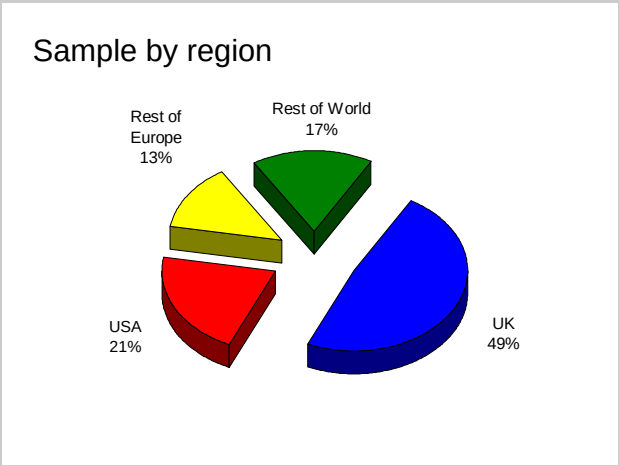
Ultimately, it doesn't matter whether any specific criterion is more or less important than any other when it comes to security best practice. There is a bigger question afoot – referring back to IT security leaders and laggards, two thirds of respondents to this study lie somewhere in between the two extremes. The most important lesson we can learn is that it will always be worth reviewing the situation any particular organisation is in, and determining what improvements can be made. This isn't motherhood, it's common sense.

As a final point, plenty can be learned from the more leading organisations but the bottom line is that security cannot be treated by tools alone. Organisations looking for a sticking plaster solution may find themselves with more cuts and grazes than those who know not to walk through the brambles in the first place.

Appendix A

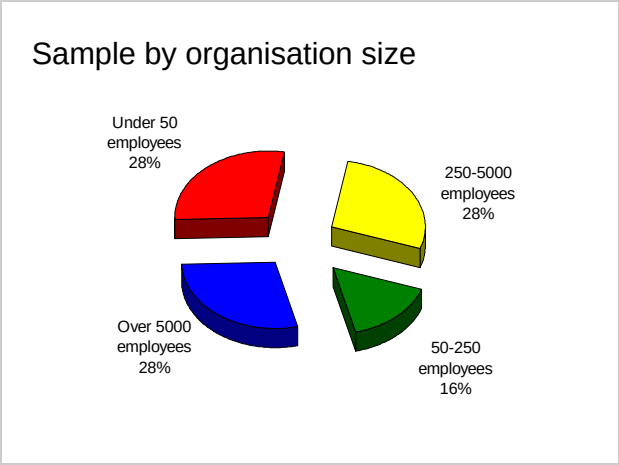
RESEARCH SAMPLE

The research sample was 1,102 respondents, distributed as shown in the figures below.



A reasonable proportion from non-English speaking countries...

Figure 15



... And a good spread across company sizes.

Figure 16

Appendix B

REFERENCED WORK

[1] “Enabling the Trusted Workforce – A balanced approach to managing people related risk”, Jon Collins and Dale Vile, February 2007

[2] “IT on the front foot – Sourcing, architecture and the progressive IT organisation”, Jon Collins and Dale Vile, April 2008

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 ITC strategy, planning, procurement and implementation. Our output is therefore grounded in real-world practicality for use by mainstream 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.