The Information Security Breaches Survey 2004 was released in April 2004 by Stephen Timms MP, the Minister of State for Energy, e-Commerce and Postal Services. The ISBS is a series of biennial surveys that are widely quoted for their statistics on the breaches companies suffer from and the controls companies apply.

There is one aspect of the ISBS 2004 survey that significantly hampers its usefulness. If this could be addressed for future surveys, their results could become very much more useful for UK plc. The purpose of this paper is to explain what is needed and why, and to encourage that improvement to be made.

THE SURVEY WITH A HOLE IN THE MIDDLE

The Information Security Breaches Survey 2004 is the latest in a series of biennial surveys that has been run by the DTI since 1991. The surveys aim to help UK businesses to understand the risks they face and to improve the security of UK plc.

There is one aspect of the ISBS surveys that significantly hampers their usefulness in this regard and that is that they fail entirely to enquire about the security threats companies are besieged by, even though it is the threats that are the causes of the incidents companies suffer. This hole in their middle could and should be filled. Future surveys would be a much greater help to security officers trying to make security improvements within their company, and would contribute to a significant improvement in the security of UK plc.

> The ISBS surveys cover security incidents and the controls people deploy, but not the threats they are besieged by. The threats are the causes behind the security incidents people experience.

THE ISBS METHODOLOGY

The ISBS surveys the incidents companies experience and the controls companies apply. It does not make any enquiries to measure, profile or quantify the security threats companies are under.

That the ISBS fails to enquire about threats is clear from a brief inspection of its structure. The main body of the ISBS 2004, after the "Headline News" summary and description of its methodology, is in three sections:

- It surveys people's attitudes towards Information Security and the effort they expend to protect themselves (pp 6-14).
- It surveys the security breaches people experience (pp 15-25). It looks at how the trend is changing, both overall and for each of the different types of breach, and it categorises the level of impact or financial pain these security breaches cause.
- Then it surveys each of a wide variety of controls people deploy (pp 25-31).

Nowhere within its pages does it report upon the threats that cause the security breaches it covers.

+44 1264 332 477; John.leach@johnleachis.com; www.johnleachis.com;

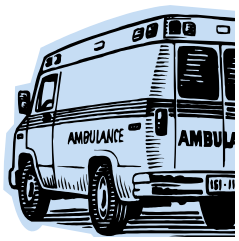
What Role Do Threats Play?

Is this a minor omission or a large hole? What role would threats play in such a survey? Is it important that the threats should be covered?

We can see that this is more than a minor omission by imagining an equivalent survey not about security matters but about, say, people having accidents on the stairs at their place of work. Applying the ISBS methodology to such a survey would produce a survey:

1. That covered attitudes towards safety on the stairs and the effort companies expend to make sure their staff stay safe:
   - How many companies think this is an important issue [p6];
   - Do people feel they know how bad a problem this is for their organisation [p6];
   - Do they tell their staff to be careful [p8];
   - Do they check to make sure their staff comply [p9];
   - Do their safety people have formal safety qualifications [p11];
   - and so forth.

2. That looked at the various outcomes of people having accidents on the stairs:
   - How many people just get an adrenalin rush;
   - How many get bruises;
   - How many break or sprain a limb;
   - How many end up in hospital;
   - How many die.



3. And that surveyed the things people do to reduce their risk of having accidents:
   - How many take the stairs one at a time;
   - How many people avoid running down stairs;
   - How many avoid carrying heavy boxes up or down the stairs;
   - How many make sure a spill gets reported and cleaned up promptly;
   - And so forth.

At no stage would this imaginary survey be measuring or profiling the reasons why people have accidents on the stairs. There is no place within the ISBS methodology where the survey would be asking, for example, whether people were falling because the stairs were too steep, or old and poorly maintained, or the steps too narrow, or too polished and slippery. Nowhere would it be asking how many times people saw others carrying heavy boxes or running down the stairs. Yet these are the threats that are the root causes of accidents.

How could a safety officer decide how best to improve safety on the stairs if he/she didn't know what it was about the stairs, its design, its condition or its use, that was causing the

+44 1264 332 477; John.leach@johnleachis.com; www.johnleachis.com;

accidents that did occur? There is no point putting up signs telling people not to carry drinks up the stairs if the main problem is that the stairs are simply rotten and falling apart.

The same situation applies for the ISBS. How can a security officer decide which of all the measures they could take would make the biggest difference to their risk levels if they have no information pinpointing which of the threats is the predominant cause of their present day risk?

How Large a Hole Is This?

It is a very large hole.

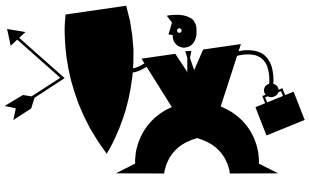
The main goal of the ISBS is to encourage and support security officers improving their company's level of security. To improve security, the officer needs to spend effort and money. To do that, the officer needs to make a convincing case to senior management that the benefits achieved will be commensurate with the costs incurred. If the ISBS is to help raise the security of UK plc, it must help the security officer to make that case.

> The security officer needs to make a convincing case in terms which relate to his/her company's particular circumstances. The ISBS survey could, and should, help them do that.

To make a convincing case, it is not necessary for the security officer to produce a formal Return on Investment (RoI) calculation. It would be marvellous if we all had the ability to perform RoI calculations for security expenditures, and it is somewhat odd to see the ISBS lament that "under half of all businesses evaluate return on investment on security spend" (ISBS 2004, p3). As anyone who has tried will know, we simply do not yet have the tools with which to perform proper RoI calculations for security expenditures.

But neither is it sufficient for the security officer just to point to what other companies do. It is not sufficient to tell a company director that "companies now spend on average 3% of their IT budget on security" (ISBS 2004, p3) even if that director currently spends only half that amount. It is not sufficient to report that "a third of large businesses have moved to use some form of two-factor authentication" (ISBS 2004, p3) to justify a proposal to spend a large sum to improve user authentication. Keeping up with the pack is not sufficient justification for spending more on security. Directors rightly insist that their security officer must do more than just follow the herd. In a well-governed company this is exactly the correct stance to take.

Common sense on its own suggests that spending more on security controls should lead to a reduction in security incidents. But the security officer needs to call on more than just common sense. They need to know where to focus their efforts to achieve the greatest benefits, and they need to substantiate to senior management that the benefits will be worth the effort. For that, they need threat data, and the ISBS does not provide them with that.



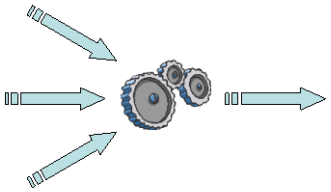
Threats cause security incidents. People put security measures in place to counter the threats they face. Their security measures are their defensive shield keeping the onslaught of attacks at bay. How can a security officer tell where their defences need strengthening if they do not know where the threats are sneaking through? They could look to their security incidents and then try strengthening all of the security measures that counter the incidents that cause the most disruption. But that approach is very inefficient and leads to a lot of effort being wasted strengthening measures that don't need to be strengthened in order to catch the ones that do.

+44 1264 332 477; John.leach@johnleachis.com; www.johnleachis.com;

A Few Simple Rules of Thumb

At a minimum, the security officer needs a few simple rules of thumb to help them work out where to focus their efforts. They need a few simple algorithms that say:

> "If the threat looks like this, …
>
> … and you are a company in this size bracket, …
>
> … then improving this given control from this level to that level …
>
> … can be expected to lead to a reduction in incidents of around X%".



Armed with that type of simple rule, the security officer could then determine what deployment level the company was on, what deployment level they needed to reach, and how much it would cost them to achieve that.

These rules of thumb could easily be compiled if the ISBS were to report on the threats rather than restrict itself to reporting on only incidents and controls. If the ISBS would show people the profile of the threats and whether the threats were changing in any particular way, people could rebalance their defences to meet the evolving threat. If the ISBS would show people the magnitude of the threats and how the threat was growing from year to year, people could decide how much they needed to strengthen their defences in order to maintain a desired level of protection.

This is what the ISBS needs to do.

An Opportunity for Improvement

This absence of threat profiling is a shortcoming that all the security surveys listed in the ISBS (Figure 36, p16) suffer from. This means that the ISBS 2004 survey is of no less value than any of the other surveys produced each year. Importantly, it means that the DTI has an opportunity to distinguish future ISBS surveys from the pack by including threat profiling. This would make future ISBS surveys very much more useful than security surveys have been in the past.

> Future ISBS surveys should report on the magnitude and profile of the threats to help people make the case for specific security improvements.

For the ISBS surveys to report on the magnitude and profile of the threats would not necessitate the DTI conducting the measurements itself. It could work in partnership with those who could make the measurements, and make their results much more widely available, just as it already works in partnership with several major security vendors for different aspects of the current surveys.

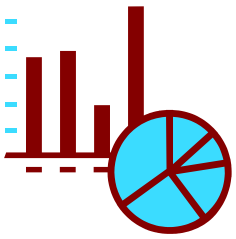
Here are three specific examples of the types of threat reports that would be helpful in this way.

Profiling the Virus Threat

Rather than just measuring how many companies experience how many virus incidents over the year, have the ISBS report on how rapidly viruses spread and whether the trend is for viruses to spread more rapidly this year than last. If viruses were spreading more rapidly, the average age of viruses in the field would be getting younger. Then have the ISBS survey how

+44 1264 332 477; John.leach@johnleachis.com; www.johnleachis.com;

frequently companies update their AV signatures. This would allow the ISBS to build a useful rule of thumb and enable security officers to determine if they needed to improve their AV deployment.



Let's suppose, for the sake of argument, that the ISBS finds that 10% of the viruses people are exposed to on a typical day are less than 12 hours old, 20% are 12-24 hours old, 30% are 24-36 hours old, 30% are 36-48 hours old and the remaining 10% are all more than 48 hours old.

The security officer can look at how frequently their company updates AV signatures and compare that with the age profile of the viruses they are being exposed to. Let's say the company currently takes 24 hours to update their AV signatures. Then they could reasonably expect to see a reduction in their level of virus incidents of around two thirds if they were to reduce that 24 hours to 12 hours. That is a specific result that the security officer could take to the IT Operations manager to get the company to improve its AV defences by a specific amount.

PROFILING THE INTRUSION THREAT

Rather than just measuring how many companies experience unauthorised access to their systems by outsiders, have the ISBS report on how quickly hacking exploits tend to appear on the Internet once a vulnerability has been announced and how quickly after that the exploits are seen in use. Report on the trends and whether exploits are appearing more rapidly this year than last, or if the number of zero-day attacks is becoming significant. Finally, have it survey how promptly companies apply software patches once they have become available or rectify the deficiencies discovered through the penetration tests they commission. This would allow the ISBS to build another useful rule of thumb, this time to do with the benefits of software patching.

Let's suppose, for the sake of argument, that the ISBS finds that exploits typically appear on the Internet within four days of a new vulnerability being published, that 10% of those exploits are detected in significant use within a month, that a further 10% are detected in significant use within three months, and that the remainder are never detected in significant use at all. Let's also suppose that the ISBS finds that exploits do not normally appear packaged in worm form for at least a month after the exploit has appeared, that 25% of worms exploit vulnerabilities that are between one and three months old, and that 25% exploit vulnerabilities that are more than three months old. And let's suppose that the ISBS shows that zero-day exploits are essentially never seen.

How would the security officer use this type of data? The security officer could look at how long the company takes to apply patches and compare that with the rate at which vulnerabilities get used in exploits or in worms. If, say, the company typically takes three months to apply software patches, they could reasonably expect to see a reduction in their level of worm infections by around 50% if they were to reduce that time to one month, and possible a similar reduction in the number of successful hacks they experienced too.

Software patching is expensive to do well and a lot of companies will not put more effort into patching until they can see there is an adequate return to be obtained. If the ISBS could provide this type of threat profile, it could make an enormous difference to the security of UK plc.

+44 1264 332 477; John.leach@johnleachis.com; www.johnleachis.com;

PROFILING STAFF MISUSE OF IT SYSTEMS

Rather than just measuring how many companies suffer from different levels of staff misuse of their IT systems, from excessive Internet browsing all the way up to computer-assisted fraud, have the ISBS report on the degree to which people at large show disrespect to authority and show themselves willing to break the rules, whether those rules be a code of authorised Internet use, a contract of employment or the Official Secrets Act. Then have the ISBS measure how much effort companies put into building their security cultures, performing security vetting or developing deterrents to influence their staff security behaviours. This would enable the ISBS to build several rules of thumb showing how reductions in internal security breaches could be achieved by improvements in internal security controls.

A recent analysis of exactly this point has shown that:

- Strengthening an organisation's security culture reduces the rate of internal security attacks more than it reduces the severity of those attacks;
- In contrast, the effects of security vetting are much more evenly balanced. Vetting leads to a reduction in the rate and in the severity of attacks, with it perhaps having slightly more effect on attack severity than on attack rate;
- Beyond a certain point, strengthening the accuracy of security vetting consumes more effort by the vetting organisation and is fairer on staff but appears to have almost no benefit in terms of the end results achieved;
- Deterrence has a strong effect on the rate of attacks but only a small effect on the severity of attacks.

The specific results suggest that strengthening the corporate security culture is the single most effective countermeasure a security officer can deploy against the internal threat. Also that a mixture of countermeasures is needed if the goal is to achieve a marked reduction in the expected severity of attacks, not just in the expected rate of attacks.

CONCLUSION

The ISBS does not currently measure or profile the security threats that are the cause of the security outcomes people experience. This leaves the ISBS, in common with all similar security surveys, telling people only what they already know from common sense alone, and unable to do much more than extol the general benefits of all companies taking more security care. If the ISBS were to report on the magnitude and profile of the prevailing threats, it would provide essential support to company security officers and contribute to a marked improvement in the level of security being practiced by UK companies at large. This would be an extremely valuable outcome and would enable the ISBS to achieve one of its central goals, to be of tangible benefit to its readers.

Information Security is fast becoming much more of an engineering discipline than the art it has always been, and engineering disciplines are driven by sound data. There is a huge need for a survey that reports meaningful threat data allowing useful results and rules of thumb to be drawn. The ISBS 2004 does not achieve that. The DTI has an opportunity to rectify that in time for ISBS 2006.

Dr John Leach
John Leach Information Security Ltd

+44 1264 332 477; John.leach@johnleachis.com; www.johnleachis.com;