



Executive Summary

Sharing of incident data with organisations who have common issues is an effective method of warning and threat assessment, and sharing good practice data helps benchmarking. Both of these would significantly increase the quality of information risk assessments.

The WARP (Warning Advice and Reporting Point) programme provides a framework and toolkit for those who wish to share information. It is supported by many important stakeholders and addresses the cost and risk of sharing.

As organisations are becoming more and more dependent on Information and Communication Technology (ICT), the information which is held and processed by these ICT systems, if stolen, corrupted or lost would have a significant detrimental effect on the operation of the organisation.

It is impossible, and would not make economic sense, to try and design ICT systems which are 100% secure and a risk based approach is preferred.

Risk is the product of *impact* of abuse and the *likelihood* of the abuse taking place, both of which are difficult to quantify.

Quantifying the *likelihood* and threat is especially difficult because no one likes talking about their own security incidents because of risk to reputation.

What is the scale of the problem?

- Much has been done by IAAC and others to try and engage organisations at board level to increase awareness of information security.
- The DTi's ISBS 2002 stated that "information security has never been a higher priority at the board level. 73% of UK businesses (up from 53% in 2000) believe information security is a high priority for senior management. Relatively few businesses are translating this priority into effective action."
- The survey outlines the reason is an under investment in IT security but arguably this is compounded in many organisations because it still sits in the '*too difficult*' category.

Issues for the Board

- Risk assessment & management are accepted tools in building effective corporate governance and managing a business. Why is it that risk assessment against information assets is often at best based on individuals 'gut feel' assessments or at worst ignored?
- All too often the question of risk assessment of your information assets is put in the '*too difficult*' category, while organisations focus on more pressing needs such as the financial realities of surviving the current economic downturn.
- This briefing paper aims to move some of the issues out of the '*too difficult*' category into the '*simple no-brainer*' category, so it would be culpable not to do anything about it, despite other business pressures.

The Information Assurance Advisory Council (IAAC) is a private sector led, cross-industry forum dedicated to promoting a safe and secure Information Society. IAAC brings together corporate leaders, public policy makers, law enforcement and the research community to address the security challenges of the Information Age.

Date for your diary: **National Resilience and e-Crime: Why Should Business Care? IAAC 4th Annual Symposium, 17 October 2003, London (hosted by the DTI)**



Questions from the management

When an organisation suffers a major security breach, especially one perpetrated on-line, one of the first questions a senior manager is likely to ask is:

Question 1 - "Are we alone, has anyone else suffered a security breach?"

Followed closely by:

Question 2 - "Why us, is it because we are more vulnerable than others?"

This tendency to compare ourselves with others is natural as it helps establish whether we have been negligent, both from a personal viewpoint and a corporate governance viewpoint. But how likely is it that these questions can be answered in a timely and detailed manner so as to be useful?

And why wait until a security breach before these questions are asked?

If you know the details of security breaches in other organisations and whether/how you are more vulnerable than others it helps you take effective and timely business decisions based on a collective experience and would reduce the risk of you suffering a security breach in the first place.

Answers to the first question provide a warning mechanism for the threat and help you judge the likelihood of a breach, which helps quantify the risk and enables timely countermeasures to be deployed. An answer to the second question would provide valuable benchmarking data which you can again use to help quantify the risk, and where appropriate, take countermeasures to reduce the risk based on the good practice experience of your peers.

So how much would you pay to have these questions answered on a regular basis and where would you go for the information? There are commercial organisations out there who can advise on these areas but it can be argued that they are unable to answer the questions completely.

How can these questions be answered in a timely and cost effective manner?

The answer is to share information with other organisations who are in a similar situation, in a manner which simply recovers the cost of the infrastructure which

facilitates this sharing. This sharing community could be based on a business sector, geographic location, technology standard, risk grouping or whatever makes business sense.

The business case for Information Sharing

Background – ICT related business cases

Business case models for investment in ICT related security are scarce, and those that exist and are effective deal with very visible impacts such as loss of employee time due to virus attacks or email spamming, which are relatively easy to quantify in financial terms, and therefore enable the calculation of a meaningful ROI.

In an ideal world, a business case for information sharing should support the business case for ICT related security which in turn needs to support the business case for investment in ICT.

Experience in the industry has shown that ROI for ICT investment should include intangible benefits as justification for financial investment.

Why is it then investment in ICT related security in many organisations comes after an incident, and those organisations which suffer regular incidents normally have an active and thriving security programme. However, it is recognised that the most effective security programmes are those supported by the board as part of good corporate governance.

The following review against typical business case headings is included as an aid to getting support for information sharing amongst senior managers:

Business strategy - Information sharing supports benchmarking which is a respected tool used by many organisations to help set and deliver their strategy.

Return On Investment (ROI) - Information sharing services, as outlined in the next section, can save money by helping to reduce the cost of failure from incidents, reduce operational costs by learning from peers with regard to what works and what doesn't and improved prioritisation/efficiency of current resources. Equally important are the intangible benefits such as increased product/service quality, increased trust/customer satisfaction and increased shareholder value protection.

Ability to deliver - The creation of an information sharing forum needs to be supported and facilitated by trusted parties - an honest broker. There is also much which can be learned from existing information sharing initiatives which can be used to help deliver.

Business readiness - The organisation taking part in information sharing must be willing to share its own information with others, as well as make use of the information it receives from others. This is an important enabler and although unlikely to involve any capital cost, it may involve a change in the organisation's policy.

Compliance - Information sharing reduces the risk to personal and company data and supports the adoption of good Information Security practice. This supports compliance with, for example, the Data Protection Act and the international Security Management Standard ISO/17799 (BS 7799).

Business values - Information sharing, as well as benefiting the organisation, benefits others and therefore supports many company values.

Risk - The risk in sharing sensitive information such as incident data is probably the most significant barrier to information sharing, but this risk can be mitigated substantially by, for example, anonymisation of the source. Members of the sharing community will therefore know the information is valid, but will not know who it came from. It is also recognised that information has different levels of sensitivity, some which can easily be shared and some which will never be shared. It is expected that information sharing communities will build trust over time and therefore share more as time progresses.

Cost estimates - The cost of information sharing is small in ICT investment terms and in most organisations would not require a rigorous business case with full ROI justification.

Ownership - This is perhaps one of the most important aspects of any business case – who will own the resulting implementation in terms of being responsible and accountable? Senior managers would need to appoint an individual to look into the business case for information sharing, with help where needed from trusted parties.

Information Sharing: A 'no brainer' solution

The National Infrastructure Security Co-ordination Centre (NISCC) is promoting Information Sharing¹ and working with the Central Sponsor for Information Assurance (CSIA) to provide assistance to anyone who would like to set up and/or take part in an information sharing community.

The concept is called a WARP (Warning Advice and Reporting Point). The initial objective of the programme is to run several pilots with central start-up funding and produce a WARP toolkit which will be freely available to

any organisation or community who wants to set up their own WARP.

The first WARP was launched in April this year for the 33 London Boroughs, called the LCWARP. The three core services being developed in response to their community needs are:

Filtered Warning and Advisory Service - where members receive only the security information relevant to their needs

Good Practice and Advice Brokering Service - where members can learn from other members' initiatives/experience (non-sensitive)

Reporting and Trusted Sharing Service - where reports are anonymised so members can learn from each other's attacks/incidents without fear of recriminations (sensitive)

Other public sector organisations are in discussion with NISCC about creating further WARPs and the CBI is helping identify WARP communities from the private sector. The WARP concept also has the support of most UK CERTS through the UKCERTs forum.

The commonly held view that people are reluctant to share is not borne out by the evidence. Senior managers from many organisations have said that if the right safeguards were provided then they would be prepared to share because they can see the benefits of doing so.

These three core services would provide regular answers to the questions posed in the previous section and more - so how much would you pay to get these answers? Depending on the size of the WARP and the level of service provided, a Member's annual subscription could be typically £5k/year, while a fully co-operative and burden sharing approach would incur no significant external expenditure at all.

IAAC Sponsors

- Anite.net
- BAE Systems
- HP Labs
- RAND Europe
- QinetiQ
- Symantec
- Microsoft

Government Liaison Panel

- Cabinet Office
- Office of the e-Envoy
- Communications-Electronics Security Group
- National Infrastructure Security Co-ordination Centre

Disclaimer: IAAC's recommendations do not necessarily represent the views of any of its members or sponsors, whether government or private sector.

¹ National Infrastructure Security Co-ordination Centre (NISCC) Information Sharing Publications - http://www.niscc.gov.uk/Information_Sharing.htm