NISCC
NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE

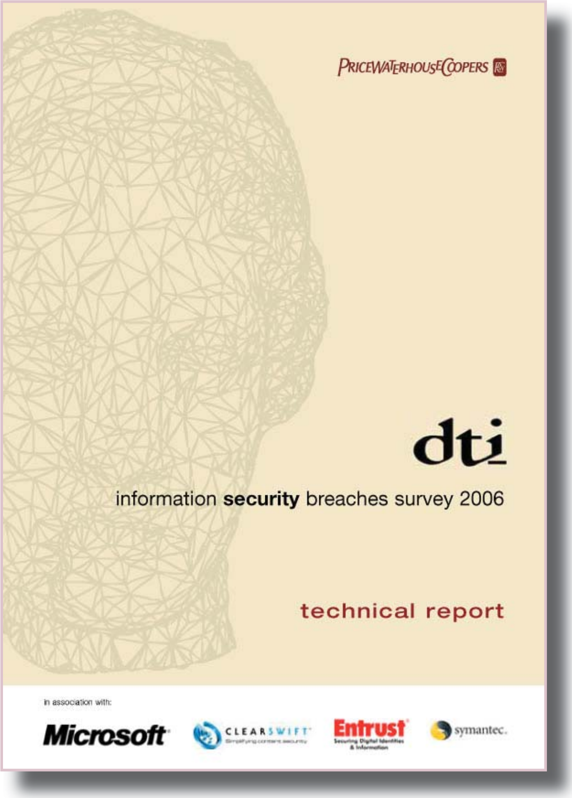
the Quarterly

In this issue:

- NISCC vulnerability work
- NISCC and NGSSoftware working together
- CIIP developments in Europe
- NISCC receives leadership award
- Experience setting up a WARP
- WARP Forum 2006
- DTI Information Security Breaches Survey 2006
- IA06 - the Government IA event

National Infrastructure Security
Co-ordination Centre (NISCC)
PO Box 832
London
SW1P 1BG
Tel:0870 487 0748
Fax:0870 487 0749
Email: enquiries@niscc.gov.uk
Web: www.niscc.gov.uk

01/06



PRICEWATERHOUSECOOPERS

dti

information **security** breaches survey 2006

technical report

in association with:

Microsoft CLEARSWIFT Entrust symantec.

Welcome to the latest NISCC Quarterly. In this issue there's an insight into how we handle vulnerability issues and a look at how we work in partnership with the private sector.

The DTI Information Security Breaches Survey is highlighted. We also visit the recent IA06 conference in Brighton, report from the last WARP Forum, and see how to get a WARP off the ground. Beyond our shores, there's a report on CIIP developments in Europe. And finally, there's a short story on NISCC's most recent award.

NISCC vulnerability work

by NISCC staff

The NISCC Vulnerability Management Team (Vulteam) has the lead for the responsible identification and managed disclosure of IT software and hardware vulnerabilities. The key to our work is trusted relationships with all areas of the community. These include vendors, researchers (both academic and independent) and penetration testing companies.

The Vulteam is constantly seeking to build on existing relationships, and also to establish new ones with companies in the private sector.

The Vulteam is currently working closely with the University of Oulu on a suite of test tools for DNS. The tools highlight a number of vulnerabilities, specifically queries, query replies and zone transfers which can result in Denial of Service (DoS) attacks. The Vulteam has distributed the test suite to more than thirty vendors. Over half of these vendors have found and patched vulnerabilities in their products. A public statement was released earlier this year, along with comments from vendors.

The Vulteam is interested in improving overall security of internet protocols and to this end we have engaged Fernando Gont, a prominent researcher, with whom we have previously worked closely. He is currently examining the specifications of IP and TCP on NISCC's behalf and it is expected that this work will be finished in the summer. We hope this will result in recommendations being made to the Internet Engineering Task Force (IETF) to alter the security specifications of these protocols enabling an improvement in internet security globally.

Moving to the future, we are developing our capability to actively engage in our own vulnerability validation and research work. We have invested in new equipment which will be put to use when we analyse Audio Format, SMTP server, SNMP v.3 and HTTP server using test tools recently acquired from Codenomicon.

Shortly we will also have our own dedicated network, enabling the team to receive vulnerability information from major international corporations who are prepared to share this information with NISCC. This together with the ability to perform our own research work will establish the NISCC Vulteam as a much more pro-active and "hands on" organisation in working with vendors in the vulnerability arena.

Finally, our framework agreement outlining our terms for sharing vulnerability information has recently been revised to include the widely acknowledged traffic light protocol (TLP). There has already been considerable positive feedback from vendors, and we are now using the latest version in our daily business.

The top cross-platform application vulnerabilities

Application vulnerabilities are the fastest growing method used by attackers.

Back-up software – the most troubling of the application vulnerabilities, because most companies store their most sensitive and confidential data on the back-up systems, and because the back-up vendors don't provide automated updating.

Anti-virus software – when software is installed as protection, users don't think it will be the path through which their systems are taken over.

PHP-based applications – this is a web application development language. A lot of php programs have critical vulnerabilities.

Database software – Oracle and Microsoft SQL Server both have critical vulnerabilities.

File sharing applications – more than a dozen peer-to-peer file sharing programs, including Kazaa to Gnutella, have multiple vulnerabilities and configuration failures that put their users at extreme risk.

DNS software – the widespread software changes addresses like SANS.ORG into numeric addresses and back. Vulnerabilities in DNS provide a great way for attackers to take over tens of thousands of powerful computers.

Media players – Windows Media Player, RealPlayer, Apple Quicktime, Winamp, iTunes all have critical vulnerabilities.

Instant messaging applications – both AIM and MSN Messenger have critical buffer-overflow vulnerabilities and all IM systems create huge vulnerabilities for companies because they allow file transfer that can often include malicious code.

Mozilla and Firefox browsers – many critical vulnerabilities have been found in these increasingly popular browsers.

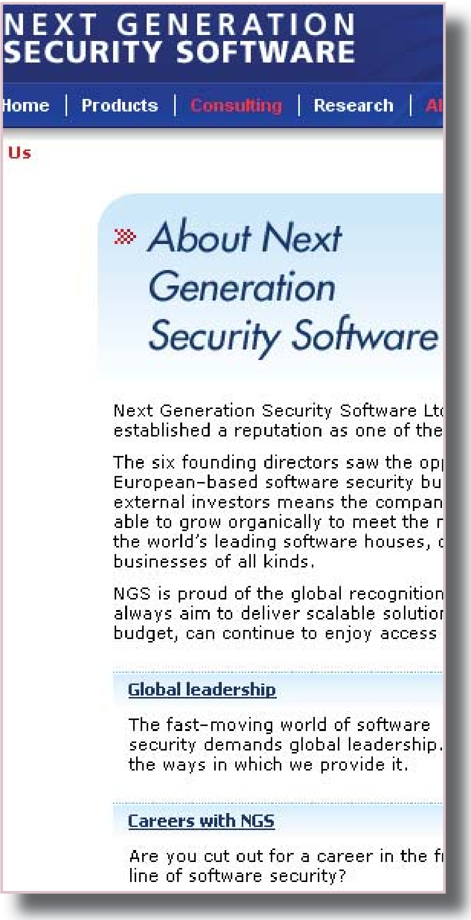
Other cross-platform applications – Computer Associates has two products on the 'other applications' list but several other vendors have products there, as well.

NISCC and NGSSoftware are team players

By David Litchfield

Next Generation Security Software Limited (NGS)[1] is a UK company based in Sutton, Surrey, which is a leader and pioneer in enterprise-level application vulnerability research and database security.

In order to help protect the UK CNI against electronic attack, NGS is providing NISCC with advance notification of software vulnerabilities in order to provide mitigation measures to CNI organisations, and is producing good practice guides on topics such as securing web applications. In addition NGS will also publish specific whitepapers through NISCC. The process of whitepaper publication has begun with the first guide on securing web applications being published and whitepapers on phishing and pharming attacks being republished.


NEXT GENERATION SECURITY SOFTWARE
Home | Products | Consulting | Research | Al
Us
About Next Generation Security Software

Next Generation Security Software Ltd
established a reputation as one of the

The six founding directors saw the op
European-based software security bu
external investors means the compan
able to grow organically to meet the r
the world's leading software houses, c
businesses of all kinds.

NGS is proud of the global recognition
always aim to deliver scalable solutior
budget, can continue to enjoy access

Global leadership

The fast-moving world of software
security demands global leadership.
the ways in which we provide it.

Careers with NGS

Are you cut out for a career in the fi
line of software security?

Bug hunters

In 2003 two of the founding directors, Mark and David Litchfield, were voted the world's best "Bug Hunters"[2]. NGS provide a range of vulnerability testing services, from automated vulnerability scanners to bespoke penetration testing, and employ several world class vulnerability researchers. As a consequence NGS maintain a database of unfixed vulnerabilities which they work with vendors to patch.

Critical vulnerabilities

One of the most critical vulnerabilities discovered by NGS in the recent past was the SQL Server discovery service buffer overflow flaw [3], which NGS worked with Microsoft to patch. Six months after the release of the patch by Microsoft the flaw was exploited via the Slammer worm, which was infamous for being the fastest spreading computer worm in history. Uniquely among security research companies, although they do put checks into their commercial database and general vulnerability scanners to protect their clients, NGS do not publish technical details of vulnerabilities until three months after a patch has been published by the vendor, thereby giving system administrators a three month period to patch their systems.

NGS is providing NISCC with advance notification of software vulnerabilities in order to provide mitigation measures to CNI organisations

Books published

NGS staff have authored or co-authored several books including, "The Shellcoder's Handbook", "SQL Server Security", "Special Ops" and "The Database Hacker's Handbook", which demonstrate a range of attacks and the methods to defend against them. The NGS web site includes whitepapers on securing both Microsoft and Oracle products, SQL injection, phishing and pharming attacks and buffer overflows and underflows.

BIOS rootkit

At the time of writing, a whitepaper on BIOS rootkit implementation and detection is to be published shortly.

NISCC looks forward to working in partnership with NGS.

[1] http://www.ngssoftware.com

[2] http://www.ngssoftware.com/brochures/SC_CoverStory.pdf

[3] http://www.sans.org/resources/malwarefaq/ms-sql-exploit.php

CIIP developments in Europe

by Home Office staff

Eurostar profits have soared over the past few months as colleagues from the Home Office and other government departments and agencies, including NISCC, have been travelling backwards and forwards to Brussels to discuss the European Commission's proposals for a European Programme on Critical Infrastructure Protection (EPCIP). The Commission's proposals first emerged in 2004 when the Commission issued a communication setting out their intention to explore the need for action at EU level in raising awareness amongst member states about CIP issues and identifying whether action needs to be taken to identify European level critical infrastructure protection (and to apply EU level standards or regulations to raise standards).

From July to December 2005 the United Kingdom held the Presidency of the European Union. This was a hectic time for officials across a wide range of government departments but, in the particular area of EPCIP, it had the advantage of allowing the UK to influence and shape Council responses to the Commission's proposals.

In December 2005, the UK published Presidency conclusions on EPCIP which established a number of key principles that we were able to agree with all 25 Member States. These were:

- a recognition that Member States have ultimate responsibility for their own critical infrastructure;
- agreement that action at EU level should add value in supporting and complementing Member States' activities;
- agreement that terrorism is the priority focus for the work of EPCIP but that an all hazards approach is a pragmatic principle that should be adopted to the protection of critical infrastructures;
- agreement that owner/operators of infrastructure, including the private sector, must be actively involved at the national and EU level.

The European Commission have been invited to present a proposal for the scope of their EPCIP. The Commission recently published a Green Paper which asked a number of questions of all Member States and the private sector to try to guide future direction of their work. The UK Government response to the Commission's Green Paper, which has been the subject of wide consultation amongst a number of departments and agencies, including NSAC and NISCC, has, on the positive side, stressed active support for a European level programme which supports exchange of good practice and clarification of definitions and principles. We also support the Commission's work in trying to identify European level critical infrastructure.

We are more cautious, however, about the potential scope of the Commission's proposals (including the potential for EU level regulation and legislation where the requirement has not been proven). We are also anxious that the proposed EPCIP should not impinge upon areas of national responsibility.

A number of Commission funded studies are collecting information on specific CIP issues, such as transport, energy and electronic communication infrastructures across Europe and we are monitoring these. While we understand the need for compilation of general information at EU level, we are concerned with the attempt to collect sensitive information on national assets.

As might be expected, there is a wide range of views and opinions amongst the 25 Member States about how the work in Europe should progress. The UK is not alone, however, in being extremely cautious about some of the Commission's proposals. The Home Office, who have the lead within Government in co-ordinating our work on EPCIP, will continue to engage with the Commission (supported by colleagues from other departments) in putting forward our position. Owner/operators and private sector colleagues are also being engaged in the process and we have established some very good links already, several of which have arisen as a direct result of the NISCC Information Exchanges.

Colleagues in NISCC will be particularly interested to learn that, at the most recent seminar on EPCIP in Brussels on 9/10 March, all Member States were briefed on NISCC's traffic light protocol for information sharing. There was widespread approval for the protocol and, subject to some further discussion in expert groups, it is likely to be formally accepted.

If you have any queries about EPCIP or would like to feed in views, please feel free to contact Gillian McGregor by e-mail at gillian.mcgregor@homeoffice.gsi.gov.uk.

NISCC receives leadership award

NISCC has received a SANS Security Leadership Award for its work on SCADA and Process Control systems. The award was presented to NISCC at the SANS Process Control and SCADA security summit in Florida on 1-3 March 2006.

2006 Process Control/SCADA
Security Leadership Award
SANS
NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE

The summit, an international event attended by over 300 delegates from 22 countries, was a non-commercial, user-to-user conference which aimed to improve the understanding of the threat, explore innovative security solutions and play a role in defining the next generation of SCADA and Process Control security capabilities. A number of pre-summit courses took place with specialists in the field providing an overview of the threats including examples of real-life attacks and information on mitigation techniques. At the summit speakers from some of the largest asset owners in the world shared details of techniques and tools that work, as well as lessons learnt, while vendors provided practical technical solutions. NISCC, which was a member of the leadership group on the conference organising committee provided a presentation on the role of governments in securing global SCADA and process control systems.

The Chairman of the US House of Representatives Homeland Security Committee's sub-committee on Economic Security Infrastructure Protection and Cybersecurity gave a presentation via DVD. He praised NISCC's work in the SCADA and Process Control field stating: "I understand that the National Infrastructure Security Co-ordination Centre in the United Kingdom has proven that information sharing does work in SCADA security."

Experience setting up a WARP

- By Dr Bob Askwith, Liverpool John Moores University

This article articulates various thoughts and experiences of the planning and deployment of a Warning, Advice and Response Point (WARP) right up to the point of active operation, or 'turning the key'. It is an individual perspective on the WARP concept, how to get a WARP off the ground and most important of all, advice on community engagement.

The problems of information security have moved from military obscurity to weekly newspaper coverage over the last couple of decades. A considerable commercial market in IT security solutions has developed, from hardware and software through education and consultancy. Something is amiss. If these technology solutions work why does the problem persist so perniciously? Statistics abound on IT security, about the number of viruses, the prevalence of Denial of Service attacks, about the huge dollar amounts lost due to incidents, and so forth. Unfortunately these figures may seem remote, generic, and ultimately not a genuine reflection of the environment one operates in. Of course the cynic would point out the raison d'etre for these surveys is really just to sell more technology solutions.

As in many areas of life, it is people that let the whole game down. End users have an endless capacity to fail to understand security and be careless; IT managers and administrators do not have enough security information to do their job well; attackers still want to break into systems badly enough that they will find a way to do so. Information security practitioners need to talk to each other and be open about what actually happens on the ground. Obviously it is not that simple.

What's missing is a culture where common interest communities help themselves by exploring security information exchange. The benefits for communities should be easy to see, an improved understanding of the immediate IT security environment, exchange of best practice, access to specialist knowledge and advice speedier response to problems. Plugging this gap with the right ingredients is a challenge.

The WARP concept developed by NISCC a few years ago to address this challenge is beginning to bear fruit for those involved. Several WARPs have been operational for one year or more, with a number about to emerge into the daylight, yet more in early gestation, and, hopefully, many just twinkle in someone's eye.

A trusted community has people at its heart, not technology, so has to be nurtured slowly. To begin trust building, the community has to readily identify itself as having a common interest, then identify the business benefit to participation. In practice the benefits of a WARP are intuitive, improved information equals improved security. A positive reaction is almost a given, which makes the task of enthusing people and getting initial buy in rather straight-forward, but quantifying the benefits into a business case is not so easy.

Typically a WARP is operated by an agency on behalf of a community, for example a regional development organisation, although communities may run a WARP for themselves. At Liverpool John Moores University, we are operating two WARPs on behalf of two regional communities; local government authorities and emergency services in the north west of England. At the time of writing we are at the transition point between planning & deployment and active operation.

A trusted community has people at its heart

The first problem to overcome when considering a WARP is identifying the right community. The experience so far tends to suggest that regional focus is helpful but this might not always be true. Where a community traditionally splits along regional lines this is perhaps obvious, and this is particularly the case for local government; many regional bodies. But for practical reasons it makes holding meetings easier for all. Face to face meetings are important for the trust building in WARPs, members get to know both each other and the operator alike.

Of course some communities are either very dense, say hundreds of potential members per city, or very sparse, say a dozen nationwide. In both cases the operator should re-examine the community. How important is geography to creating this community? Should the sparse one be expanded or merged with another? Should the dense community be split into more fine-grained communities?

The other major issue in identifying a community is to be confident that these organisations would be willing to or at least that there are benefits for them to work together. Competitive pressures may prove an impediment in trust building, but then this is the reason people don't talk to each other about security already.

In both our early WARP development experiences we were able to identify a champion on the inside who could both advise us on how to engage the community, as well as help us to understand what the community would gain most from WARP. Many of the existing WARP communities are similar not only in their nature of business but also in their security needs and capabilities. Some communities will be typified by employing dedicated security personnel, other communities may defer security to systems administrators, or in extreme cases have no identifiable staff responsible for security. Some communities may already have strong control of their IT systems and good relationships with vendors and other organisations involved in security such as NISCC. Others may feel very much on their own and a little helpless. An insider is crucial to helping you understand the nature of the community, including determining if it is the right one.

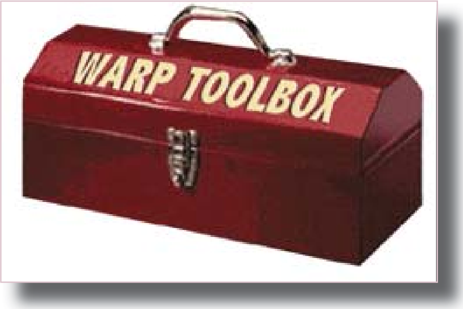
If the operator is happy to move forward with developing their WARP they need to begin to engage their community. There are two important hurdles to jump at this stage; for each member the operator needs to identify the best person to engage with, and then to sell the WARP idea to these people at a forum meeting. The right person to engage with is the person responsible for security within that member organisation.

A means to connect with the right personnel is to discuss conducting a presentation as part of a meeting of relevant professional associations, e.g. SOCITM, which members regularly gather at. We used this method successfully with a regional e-Government group association

The WARP concept is easy to understand but adapting that to a community and adding detail can prove a difficult task. There are a number of pitfalls to beware of when 'selling' the WARP. Do not assume the WARP concept is obvious to others. A WARP is quite likely to be very different to what many practitioners expect. Putting too much stress on particular aspects of the WARP may leave the wrong impression. Don't let anyone think you are selling a product or a normal service. It is community building and information exchange that make the WARP attractive in the long-term, but it is the services in the short-term that are easier to demonstrate and catch the eye of potential members. If members think they are having a product sold to them, they will become reluctant and will leave with the wrong impression.

Take for example the Filtered Warning Service (FWS), which most WARPs use as the starting point of their operation. The benefit of the service may seem obvious; the operator spends time collecting security warnings and filtering them for the community. Members receive selected warnings, and they arrive in a consistent and friendly format, therefore saving time and improving security. Operators link with other operators to share warnings to improve timelines. FWS is more than just forwarding Microsoft bulletins; operators use their resource to seek out the best security information and share that information. Members are encouraged to interact with the process, and the wider WARP community supports each other. Filtered Warnings should enhance the ability of an organisation to learn about security problems.

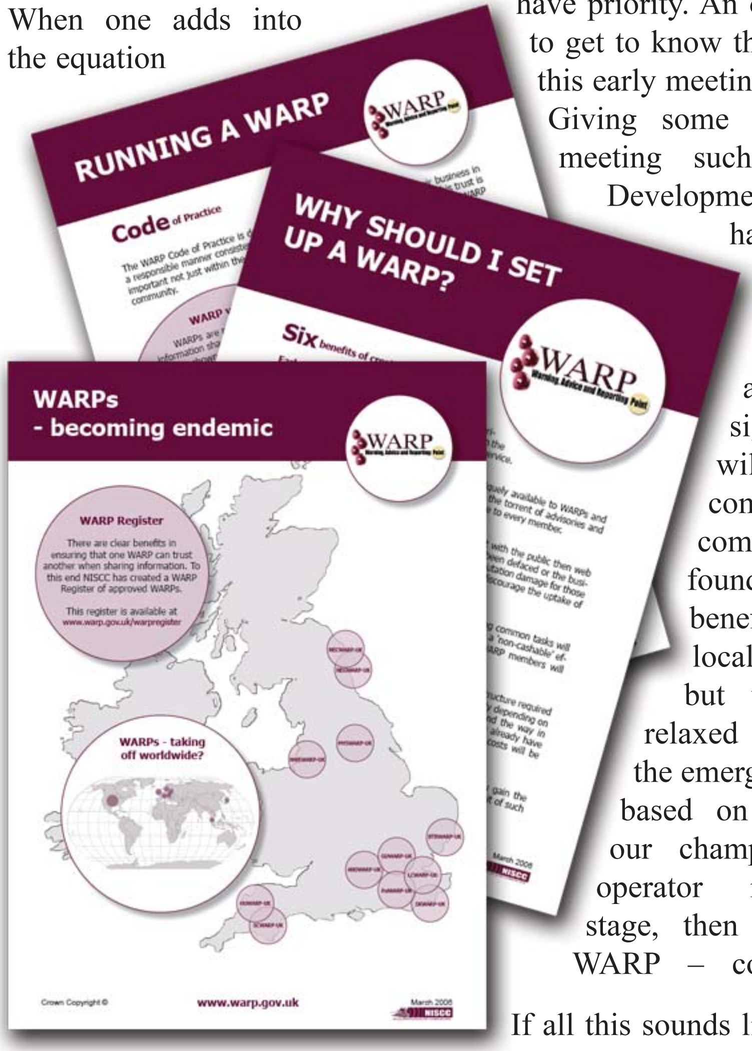
If an operator is now committed to developing the WARP for the community they should ensure that funding is secured. This will depend on who the operator is and how they normally find funding for projects. What others have typically sought is twelve months worth of seed funding being replaced by a member subscription model after that. Providing the service for free to members for the first twelve months may give just enough encouragement for members to buy-in. More importantly it gives a whole twelve month window to build up the experience of operating the WARP, including getting to know the community issues, and a chance to build the community up to a sustainable level and begin the trust building process. When remaining members are invited to join, especially if they had been reluctant to begin with, they can hopefully witness the benefits of the trial stages.



If, like most WARPs, the initial focus is on Filtered Warnings then some IT infrastructure is needed and personnel willing to fill the driver's seat identified. Details about the recommended IT infrastructure can be found in the WARP toolbox. The day-to-day running of the WARP does not require a technical wizard but someone with a strong IT background and reasonable security knowledge is essential as is someone who can be independent and contribute ideas. While different WARPs may vary in their personnel, we operate with full-time cover from technical operators and myself as part-time project manager. We have allowed the operators the space to concentrate on becoming experts in the technical issues, while in my role as project manager I guided the development, dealt with the community, other WARPs and NISCC, and, of course, kept one eye on the budget. The exact cost of running a WARP has proven difficult to assess, since the existing operators have generously contributed unaccounted-for time in order to get the WARP programme moving. A figure of £50,000 has been suggested to set up and operate a WARP for 12 months.

Getting the timing right can be

a challenge. It makes no sense spending lots of money on hardware and software if a WARP is shelved because of a lack of interest. Similarly, if community engagement activities begin too early then members may experience a period of waiting, which in the worst case can damage operator reputation, and therefore trust – before the WARP has even begun! When one adds into the equation funding processes and the inevitable time lag, frustration could be the only thing in good supply. Consultation with fund holders regarding any plans for WARP development may prove beneficial, by determining the likelihood of success and timescales involved. Ideally an operator should begin to implement their infrastructure prior to the first wider engagement meeting. If everything is working then the FWS can be demonstrated and even if it isn't plenty of time is still available to solve the remaining problems while you convene a trial member group meeting.


RUNNING A WARP
Code of Practice
The WARP Code of Practice is
a responsible manner consiste
important not just within the
community.
WARP
WARPs are
information sha
WHY SHOULD I SET UP A WARP?
Six benefits of
WARP
WARPs
- becoming endemic
WARP Register
There are clear benefits in ensuring that one WARP can trust another when sharing information. To this end NISCC has created a WARP Register of approved WARPs.
This register is available at www.warp.gov.uk/warpregister
WARPs - taking off worldwide?
Crown Copyright ©
www.warp.gov.uk
March 2006
NISCC

With everything in place the operator should invite the trial member group to meet together to consider aspects of the WARP that have priority. An operator needs to get to know the members so this early meeting is important. Giving some status to the meeting such as 'WARP Development Board' and having proper minutes and actions, may give out appropriate signals, but this will vary from community to community. We found this approach beneficial with local authorities, but took a more relaxed approach with the emergency services, based on advice from our champions. If the operator reaches this stage, then they have a WARP – congratulations!

If all this sounds like a like hard work let me say that it would be were it not for one last ingredient – yes, I have left the good news until the end. A considerable amount of the groundwork has been done already and is openly available for any operator to use. The WARP toolbox contains a mountain of documentation contributed by other WARP operators that help the newcomer. Operators are encouraged to contribute to the toolbox in as many ways as possible. Speaking as an academic, I find this the most inspiring aspect to WARP, rather like an open source software project. The collaborative nature mark WARPs out as an unusual programme – one with a very promising future.

In a nutshell

1. If the community is right, then getting initial buy-in should be easy
2. Work initially with an insider who can act as a champion for the WARP
3. Build a business case that is tailored toward the needs of the community
4. Locate a forum to introduce potential members to WARP and the business case
5. Plan carefully, once engagement begins you need to keep momentum
6. The wider WARP community is a great asset, enhanced by contribution

WARP Forum 2006

The second annual WARP Forum took place on 15th March at the prestigious headquarters of the Institute of Mechanical Engineers, Birdcage Walk, London, overlooking St James' Park.

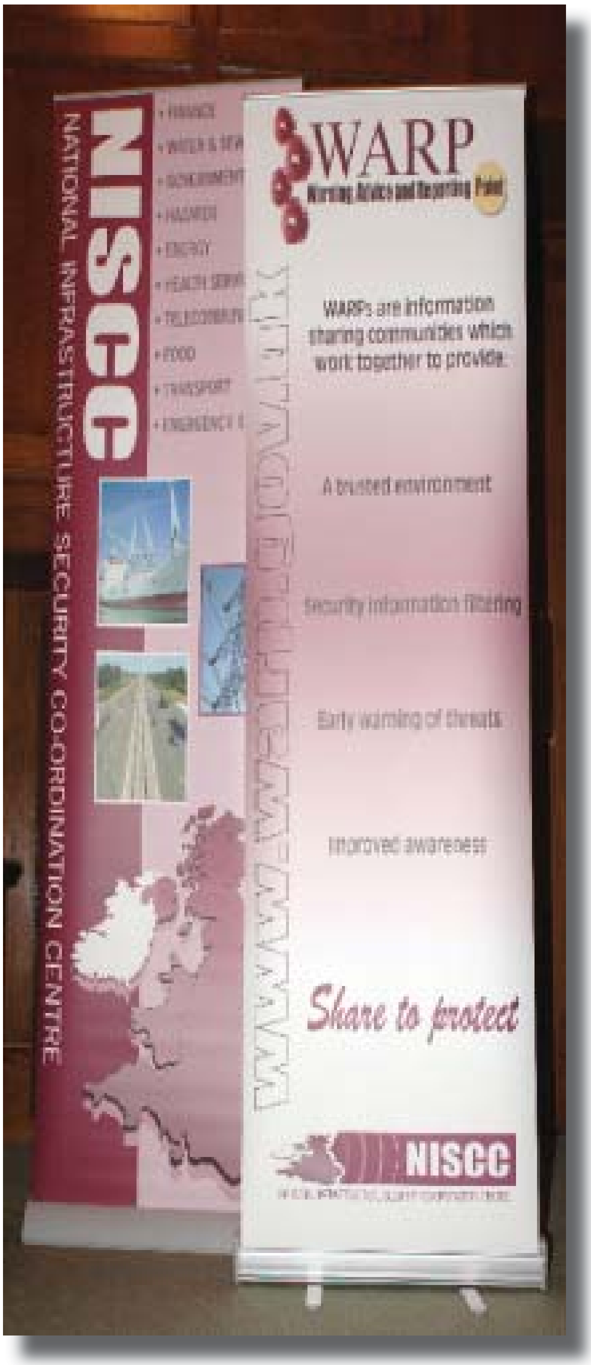
The event was attended by more than 100 delegates from various regions and countries including the Netherlands, Lithuania, Ireland, Australia, New Zealand and America. Representatives from the European Network and Information Security Agency (ENISA) also attended.

The event was opened by NISCC's Deputy Director (Outreach) who emphasised the importance of trust at the heart of the WARP model.

The NISCC Head of Information Sharing outlined some recent developments and successes, then invited the workshop chairs to give a two-minute 'advert' for their workshops so that the audience could choose which to attend, 'on the spot'. The entertainment and information values were high and stimulated extra commitment from delegates. The workshops were lively and successful, and the plenary feedback sessions were equally valuable and lively.

SANS director, Alan Paller

Alan Paller, Director of Research at the SANS Institute provided the keynote presentation, and acted as 'commentator' on the proceedings, visiting many of the workshops. His concluding address delivered valuable observations and insights, in his inimitable professional and entertaining style.


NISCC
NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE
WARP
Warning Advice and Reporting Point
WARPs are information sharing communities which work together to provide
A trusted environment
Security information filtering
Early warning of threats
Improved awareness
Share to protect
NISCC

Feedback from the Forum indicated that the workshops were well-received and provided for more stimulating debate than presentation sessions alone. Delegates new to the WARP concept appreciated the opportunity to network with those who had already set up WARPs, in particular receiving advice on lessons learned and management buy-in.

Delegates agreed that the day had provided plenty of food for thought and offered many ideas for discussion, and the overwhelming majority were enthusiastic to attend the next WARP Forum in 2007!

To keep abreast of WARP developments and for news of the next Forum, visit the WARP website (www.warp.gov.uk), or subscribe to the WARP Newsletter by emailing: subscribe@list.warp.gov.uk

Business gets underway

DTI Information Security Breaches Survey 2006

The full Survey was launched by Alun Michael, DTI Minister for Industry and the Regions, at Infosecurity Europe on 25 April. Some headlines stand out. Overall, the news is mixed - virus infection remains the main cause of security incidents for UK companies. However, most companies use anti-virus software and infection rates have dropped by roughly a third since 2004 when the Survey was last conducted. The threat is changing – in 2004 the picture was one of a small number of viruses, eg Netsky, dominating; now the nature of viruses, and the motivation of their writers, is different, witness the botnet threat. Spyware is an increasing problem and a quarter of UK businesses are not protecting themselves adequately.

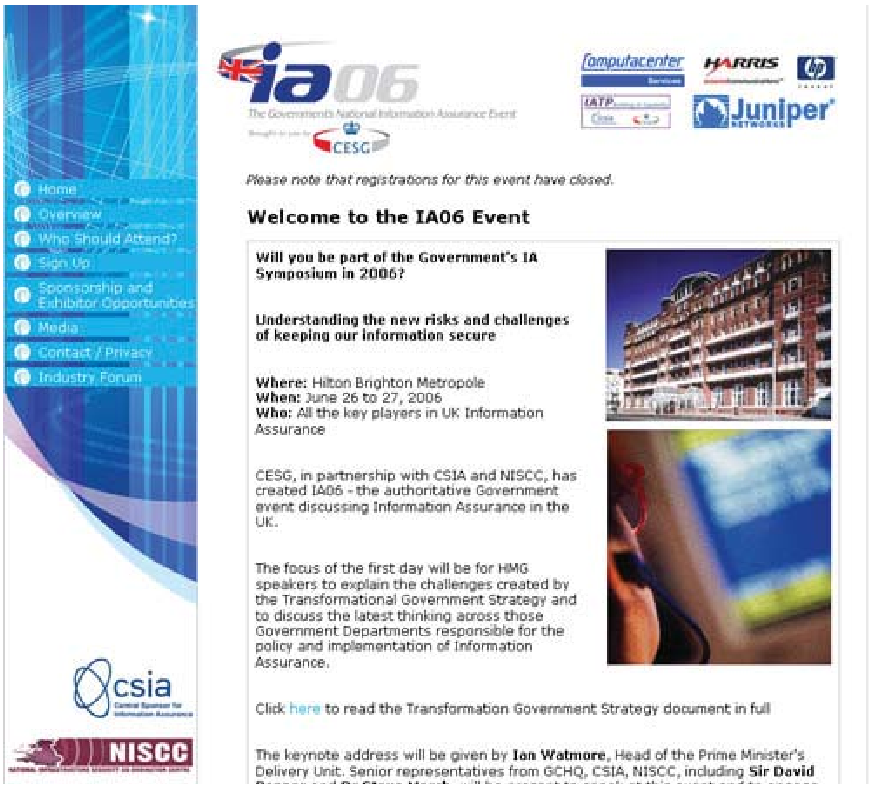
Identity and Access Management is another area where statistics are available. Identity management related incidents are consistent with the previous Survey, although large companies saw a slight rise in incidents with one in five experiencing unauthorised access to data by staff. While incidents of fraud are low, when they do occur the impact tends to be greater than other types of security breach in terms of damage to reputation, adverse media coverage and remediation costs. More UK businesses than ever are using strong authentication techniques such as software tokens or digital certificates. Software tokens in particular have been adopted by many firms as a cheap way of increasing security. Single factor authentication is still prevalent however with four fifths of companies relying on passwords alone.

Factsheets on Viruses and Malicious Software and Identity and Access Management have also been released (see www.security-survey.gov.uk).

IA06 - Government IA event unveiled

CESG, NISCC and CSIA hosted IA06 at the Hilton Metropole in Brighton from 26-28 June this year. This prestigious event – the first of its kind - brought together the major players in Information Assurance from senior Government decision-makers and influencers to key industry figures and leading academics.

Under the headline "Understanding the new risks and challenges of keeping our information secure", IA06 was chaired by Sir Edmund Burton, with keynote speeches from senior figures across Government and Industry. This invitation-only event brought together around 500 delegates and 25 exhibitors under one roof in comparative privacy, and the speaker line-up created some stimulating discussion over the two days of the conference and the follow-on industry forum.



Please note that registrations for this event have closed.

Welcome to the IA06 Event

Will you be part of the Government's IA Symposium in 2006?

Understanding the new risks and challenges of keeping our information secure

Where: Hilton Brighton Metropole
When: June 26 to 27, 2006
Who: All the key players in UK Information Assurance

CESG, in partnership with CSIA and NISCC, has created IA06 - the authoritative Government event discussing Information Assurance in the UK.

The focus of the first day will be for HMG speakers to explain the challenges created by the Transformational Government Strategy and to discuss the latest thinking across those Government Departments responsible for the policy and implementation of Information Assurance.

Click here to read the Transformation Government Strategy document in full

The keynote address will be given by **Ian Watmore**, Head of the Prime Minister's Delivery Unit. Senior representatives from GCHQ, CSIA, NISCC, including **Sir David**

Day one focused on the UK Government and policy overview, with a special session on the US perspective. Day two moved the emphasis onto the industry dimension and included keynote addresses from Sir Peter Erskine (Chairman and CEO of O2), Sir David Brown (Chairman, Motorola), Stephanie Daman (Head of Information Assurance, HSBC) and other leading industry figures.

Critical to the success of this event were detailed working groups covering crucial topics as diverse as Risk Management, CNI-Partners in Protection, Business Continuity, Future Assurance, Availability and Confidentiality, Research and Development, and IA Professionalism. NISCC staff worked closely with the organisers to help create this unique event.

Space and time was set aside for private discussion and networking and a gala dinner on the first evening, with a celebrity guest entertainer.

The Industry Forum on Day Three offered the opportunity for Industry and Academia to work with IA experts through many of the issues raised in the main conference and to consolidate the conclusions from Days One and Two. In addition it will act as the launch pad for a number of new products and initiatives.

An exhibition ran throughout the event, showcasing Government and Industry products and services. The exhibition offered an ideal opportunity for networking that was backed up with designated informal areas and social events.

IA06 lived up to the promise of an exciting benchmark for future Government-sponsored IA events.

NISCC

NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE