

Working with Warps

Warning, Advice and Reporting Points are becoming a significant force in IT security, writes SA Mathieson

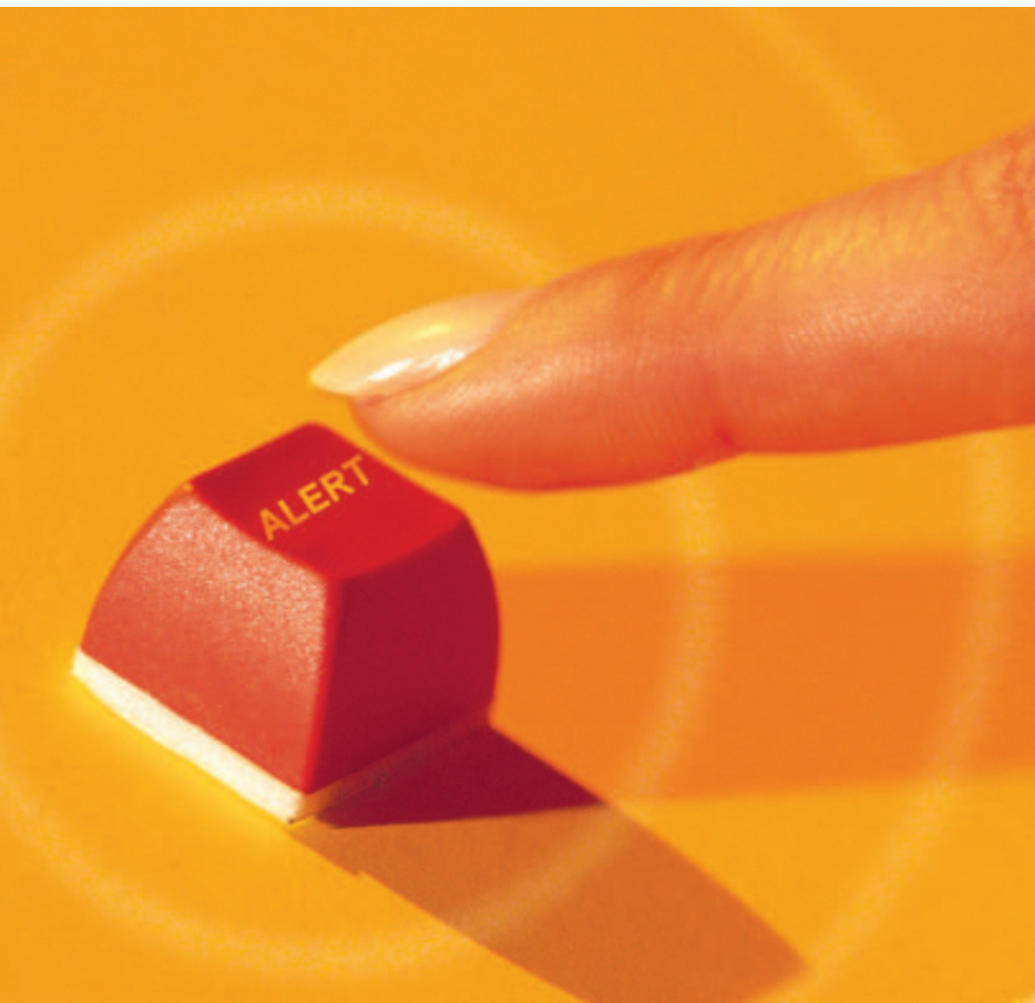
The first Warning, Advice and Reporting Point (Warp) appeared in 2003, run by the London Connects group of local authorities in the capital to share information on IT security risks, and now includes 31 of the 33 authorities. This year, the pace has been quickening, with the official number of Warps growing from 10 at the start of the year to 19 by mid-November.

This growth is partly due to central government funding for those English regions without a Warp to establish one. But it also reflects the fact that those involved believe the model, created by the National Infrastructure Security Co-ordination Centre (NISCC) to help protect critical national infrastructure, works in getting members to trust each other.

“NISCC’s vision is to create a resource, the Warp toolbox, to make Warps self-starting,” says John Harrison, an independent consultant who has worked on Warps for NISCC for three years. The toolbox is freely available at <http://www.warp.gov.uk>. “It’s a self-help community, really, so it can be made extremely cost-efficient. It doesn’t require a dedicated team full time - it leverages the power of its members.”

Harrison says the three aspects of a Warp require increasing amounts of trust and commitment, but one leads naturally to the next.

“The filtered warnings are a no-brainer, but it starts the community,” he says. “Advice brokering takes it



further." When these two are in place, members are comfortable enough to report to the group their own IT security problems with confidence: "It enables you to get information you couldn't buy commercially," he says - and discussions must not get too commercial under NISCC's code of conduct for the Warps it approves.

The speed with which IT security problems appear actually helps Warps, Harrison adds. In physical security, vulnerabilities might appear every few months: "In the electronic world, it's daily. It helps to keep the community going," he says.

Natasha Stonestreet, information security officer for Kent CC, helped establish the SecureKent Warp, which involves the 14 organisations in the Kent Connects partnership: the county, districts, Medway unitary and the county's fire and rescue service. Work started in 2003, with the Warp going live in January 2004.

"It took a little bit of time for people to trust us enough," says Stonestreet - around a year, she reckons. "Now, people are happy to share things openly."

Information is shared purely between members of Kent Connects, increasingly at meetings held to run the general partnership rather than specific ones for SecureKent.

Staying small

The relatively small number of people involved is important to build trust: there are about 100 members, with three to 15 people from each organisation, although this is planned to grow. Stonestreet says that Kent is a good size for a Warp, although aspects of the system, such as filtered warnings, could be run through a single Warp for all local authorities.

"The other side is the advice brokering and trusted sharing. The whole of the UK, all the councils sharing, just wouldn't work," she adds. "People don't trust that their information would be kept anonymous. You'd get break-out groups."

Keeping things at a county or regional level makes it much easier for everyone to trust each other, particularly as in Kent when they already share infrastructure.

John Harrison says that 30 to 50 is a good number of organisations to involve in a Warp, although this can go higher for smaller bodies, such as small businesses, to allow economies of scale. He adds that local authorities are ideal for Warps: "They all share a role, yet are all autonomous."

Peter Wood, chief of operations for

IDC highlights the human factor

Organisations are placing trust in hardware and software to solve security problems while ignoring the role of human behaviour, according to a new report.

The third annual Global Information Security Workforce Study, sponsored by the security certification organisation (ISC)2 and carried out by IDC, describes this as the "elephant standing in the room" for most organisations. It highlights the fact that a successful information security approach is as much about people and processes as IT products like intrusion detection and firewalls.

It also identifies a problem that most organisations have minimum communication mechanisms for their security policies. These take the form of emails or an intranet for a handbook and policy deployment, and in some cases organisations still chase their staff for signed policies, thus wasting untold time and money.

Any realistic assessment of these methods will confirm their weakness in the face of legal or regulatory scrutiny, says the report.

The IDC ranks the factors affecting information security professional's ability to properly protect and secure the computing infrastructure and its resources from breaches, misuse and abuse. The two most important factors are management support of security policies, and users following security policy.

There is unanimous acknowledgement from professionals in the report that "technology is only an enabler, not the solution, to executing a sound security strategy and supporting a well defined and well articulated risk management programme where everyone shares responsibility".

infosecurity consultancy First Base Technologies, says the Warp model can be compared to other ways of sharing security problems. "CERT (run from Carnegie Mellon University) is probably the most well recognised and well known alternative for bug reporting, but this is more proactive," he says, as Warps allow problems to be discussed before solutions are known. "You need a trusted environment to do it in," he adds, otherwise those seeking to cause damage could make malicious use of weaknesses. "This is about trusting each other."

Wood says that it is increasingly difficult for organisations to cope with all the potential sources of information on IT security, and creating a filtered version for that organisation makes a lot of sense.

"The whole of the UK, all the councils sharing, just won't work"

"If there's something you can trust, it will help organisations a great deal," he says, but adds: "Whether it will work is another question."

A problem with the Warp concept, Wood says, is that it depends on the person or people within the organisations running it - and given that Warps tend to be small scale, this can be just one or two.

"If you're going to do it, you need to do to it properly," he says. "If people are

going to trust it as a major source of information, it has to be up-to-date, and like any major business process you can't just rely on one person."

Natasha Stonestreet says SecureKent started with one dedicated manager, but has moved to two people working part time to split responsibility. It has taken other steps to make it robust.

"We realised the best way for it to be ongoing was for those who use it to put bits in," she says. One or two people from each member organisation have editor privileges, allowing them to add news items.

Another way in which Warps are becoming more robust is through the software having the ability to syndicate another Warp's warnings if the manager is away or unavailable. This is becoming easier, given the fact that the concept is spreading.

New Warps

As well as being used by local authorities - regionally, and in a specific one for users of Anite's software - and in the private sector, the Police IT Organisation opened a Warp in January 2005, while NHS Connecting for Health is in the process of doing so. John Harrison says a central government department will shortly announce its own Warp, which will be run by its outsourcer. Meanwhile, a Warp established for schools in Devon is a model which could be adopted elsewhere.

Mark Brett, who established the first

An Oasis for emergencies

Handling emergencies effectively requires cooperation between many different organisations. But as reports on recent emergencies, such as last year's bomb attack in London and the New Orleans flooding, have highlighted, this can be a real challenge.

The European Oasis project aims to change this by developing an IT framework based on open and flexible platforms and standards. By implementing a European wide disaster and emergency management system, the aim is to provide effective ways for communication and data sharing between different civil protection organisations.

The first trials of the Oasis (Open Advanced System for Disaster and Emergency Management) system took place in September, at Cranfield University's Resilience Centre, with users from emergency services and civil organisations.

Oasis aims to modernise the whole process of information flow in the command and control systems set up to support rescue operations in the case of large scale emergencies, such as the New Orleans flooding or the Buncefield oil depot fire. It has been put in place as part of a European initiative to improve the use of IT within civil protection organisations, after a review of civil protection capabilities highlighted the need for greater use of IT. This is now happening at a regional and national level in many EU countries, but needs to be enhanced at a European-wide level in order to provide better inter-agency communications.

The technology being used in Oasis is based on service oriented architecture (SOA), developed specifically for crisis management. The aim, according to Andy Baslington, project leader for BAe Systems, is to enable different agencies from different countries can use their own systems and technologies and combine them via Oasis.

"This will transform the way emergencies are managed," comments Baslington.

We are trying to see how SOA could apply to crisis management," says Nigel Wheadon, technology leader at BAe Systems Advanced Technology Centre, which one is of the lead players in the Oasis consortium. He says crisis management has tended to lag behind technology developments.

"These guys are used to phones and writing things down," he says. "We want to look at new interoperability standards for information exchange, in order to automate far more of the procedures involved."

The Oasis trial in September demonstrated the system in use to deal with a fictional emergency - a plume of chlorine gas from southern England hitting the coast of northern France. A UK based team of emergency workers shared more than 150 separate pieces of information with their French counterparts at EADS in Paris, using only the Oasis software and tools.

Also on trial was a prototype instrument, the tactical situation object, that delivers messages in icons and codes, allowing cross-border teams to share maps and diagrams.

Oasis brings together partners from 10 European countries, including EADS, Ericsson, Mediumsoft, Edisort and the Russian Academy of Sciences. It aims to pool the capabilities of each of the partners to produce an IT framework that will minimise the problems of diverse agencies having to act together, each with their own language, culture and technology.

Warp at London Connects and is Socitm Information Age Group's lead officer for information management, says the new regional groups set up this year with money from the now defunct Office of the Deputy Prime Minister are finding their feet.

"They've all got a pulse," he says, although work on establishing them continues in the east and south-west regions. "Every local authority has access to a Warp if they choose to," and

around one-third of those in England are doing so.

Of those not involved, he thinks some are too small to have an officer responsible for IT security, while others have outsourced their computing. But Brett says such authorities can still benefit from joining Warps, and members are being asked to bring staff from neighbouring non-member authorities to meetings. Overall, he says: "It's a really good example of a




shared service," a current central government enthusiasm.

First Base Technologies' Peter Wood says that councils seem to be doing well on securing its information, and Warps are an example of this.

"At the risk of sounding sweeping, the infrastructure models in local government are clearer, as they think about information categorisation and distribution, having thought about Freedom of Information," he says. Already completed work on understanding what data an organisation holds can then help in deciding how to secure it.

Commercial organisations, which are not subject to the Freedom of Information Act and may be less likely to receive queries on what personal data they hold, may not have done the same amount of work in this area. However, Wood says that some companies are adopting the Warp concept.

"In very switched on organisations, such as in the financial sector, you are seeing people doing the same work, definitely. It's not radical. What is good about this is formalising it." 

** SecureKent is holding a Hands On Workshop in London at the Holiday Inn hotel in Bloomsbury on 25 January, aimed at those within local authorities, the NHS and schools thinking about Warps. More details: www.securekent.com.*