

WARP Case Study Experience setting up a WARP

About the author:

Dr Bob Askwith is a Senior Lecturer in the School of Computing and Mathematical Sciences at Liverpool John Moores University. His research interests are in computer/network security and mobile computing. Bob is the project manager of two WARPs operated for communities in North West England. NWEWARP is operated for Emergency Services and NWGWARP for Local Government authorities, in partnership with the North West e-Government Group (NWeGG).

Email - R.J.Askwith@ljmu.ac.uk

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

As the problems of information security have moved from military obscurity to weekly newspaper coverage over the last couple of decades or so, 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'être* for these surveys is really just to sell more technology solutions.

Well, 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 more just a twinkle in someone's eye.

A trusted community has people at its heart, not technology, so has to be nurtured slowly unlike an off-the-shelf technical solution that activates at the double-click of a mouse. To begin this trust-building process, the community has to readily identify itself as having a common interest, then identify the business benefit to participation. In practice the benefits of 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.

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, forums etc. exist for within the region containing representatives from our communities. 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? With the luxury of many WARPs to choose from a member could move from one WARP to one they felt more identified with.

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. However, an outsider really needs approach their community assuming that all is not as it seems and have this as one of the principal goals in the next phase of developing their WARP: connecting with the community.

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, others 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. This might not be the person the operator finishes up corresponding with, but is crucial to getting the right level of support and commitment. Dealing with the right person also helps in the sense they are more likely to understand the implications of WARP within their 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, and while we had neither representatives from all potential member authorities or perhaps the right people from within all the authorities represented we did get enough on board at that stage to move forward, with the benefit that this was a painless and efficient mechanism to use.

The insights gained from working with an insider should prove invaluable in preparing for this initial engagement meeting. 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. Community building and information exchange makes 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, 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 a considerably smaller proportion of the warnings that the operator has handled, and receives them in a consistent and friendly format therefore saving time and improving security. Operators link with other operators to share warnings to improve timelines. Naturally, many organisations already perform this operation internally for themselves, so it appears much like a duplication of effort at first glance. Worse still, when a vendor releases a warning the organisation may receive it at the same time as the WARP, i.e. before the WARP forwards it. So the benefits are subtler than they look. The community aspects, leading to trust and information exchange should be the main incentive. Filtered Warnings 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, but 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 carrot 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 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.

With funding in place the operator needs to put the final pieces of the jigsaw in place. If like most WARPs the initial focus will be 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, but amount to one or two servers and a small amount of software such as a database and web server. 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, not only because each one is different, but also that existing operators have generously contributed unaccounted-for time and resources in order to get the WARP programme moving. Figures in the range £30-50,000 have 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 the community were not interested. 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. Engaging with a community insider as the starting point also gives the opportunity to begin a funding process as soon as it appears the community is the right one; if funding fails then at least a whole community haven't been let down. Ideally an operator should begin to implement their infrastructure prior to the first wider engagement meeting. If everything is working then the Filtered Warnings 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.

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 these early meeting as 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 WARP out as an unusual programme – one with a very promising future.

In a nutshell:

1. If the community is the right, 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

18 May 2006