

CSIRTs and WARPs: Improving Security Together

WARPs (Warning, Advice and Reporting Points) and CSIRTs (Computer Security Incident Response Teams, also known as CERTs — Computer Emergency Response Teams) can be effective approaches to different aspects of the problem of computer and network security. Neither has to be resource intensive: they should be viewed as opportunities to use organisation and processes to make the best use of limited resources. This paper compares the two models and suggests how using both together could further increase efficiency and effectiveness.

What is a CSIRT?

The CSIRT model was created in response to the first Internet worm in 1988. This worm overwhelmed mail servers, isolating the people working to resolve the problem in different Internet-connected sites. The original CERT® (the terms are used interchangeably) was therefore created by the US Government to coordinate the response to future Internet incidents. As the Internet has grown, more CSIRTs have been created to provide incident coordination for national research and education networks, for governments, for companies and other organisations, and for users of particular software or hardware products.

Each of these teams has a responsibility to its own constituency and also to the rest of the Internet to ensure that security incidents within the constituency are contained and resolved. External parties often report incidents to a CSIRT rather than trying to find the correct contact within the constituency. A CSIRT's constituency may be large and will usually have designated contact points for organisations or departments. CSIRTs have different degrees of authority but they all tend to be placed above or to one side of the constituency they serve, often in a security or operations team, rather than within it.

CSIRT staff need good technical skills in order to understand quickly the nature of a problem and suggest how it may be contained and remedied. They must also have good inter-personal skills: most of the people CSIRTs deal with have just suffered a security incident and may be in a distressed state. Many CSIRTs also investigate and describe security vulnerabilities, and some produce extremely good documentation. However, most CSIRTs have a large and varied constituency, so it is rare for these documents to be tailored to specific groups of users or distributed to specific individuals. For the same reason, although CSIRTs try to deal individually with constituency members who have general security questions, limited resources often restrict such advice to pointers to published information.

What is a WARP?

The WARP model was developed by the UK's National Infrastructure Security Coordination Centre (NISCC) to address a different security problem: encouraging users to learn from and apply the good practice and security information that is already available, either in published form or within communities and interest groups. WARPs therefore aim to reduce the number of security incidents, while CSIRTs' main aim is to reduce the impact of those incidents that occur.

WARPs are best created in small communities, to encourage the flow of information about security issues into and within the community. This information may include common problems and solutions relevant to the particular community, good practices in operation and design, and warnings and solutions for incidents and vulnerabilities. Where incidents occur within its community a WARP is likely to share information, with the original source anonymised when required, to help others avoid or resolve the same problem.



Most WARP members join the community by choice, so are more likely to contribute to its success both by contributing and acting on information, whereas CSIRTs whose constituencies are imposed by organi-

sational or network boundaries may find their members are more passive. WARPs are unlikely to be seen externally as responsible for their communities, though community members may, of course, feel that their WARP has some responsibility to them.

How can they work together?

The different skills of CSIRTs and WARPs and their relationships with their communities suggest a number of ways in which they can collaborate. It should be noted, however, that both types of team are generally funded to provide service to a specific community and opportunities to work outside that community may be limited or have a lower priority.

All CSIRTs would like preventive advice to be more widely adopted. WARPs, who have a closer relationship with their communities, should be able to achieve this. The most obvious area for collaboration is therefore in the sharing of information about preventive measures. Whether CSIRTs develop their own information or collect it from other public sources, agreeing to provide this information to nearby WARPs should benefit both parties. This may be done manually or using software designed for this kind of information sharing. As the relationship develops, a WARP may help a CSIRT provide better information, either by suggesting information that would be helpful to its community, or by passing on lessons learned within the community that the CSIRT may be able to document and share more widely. Such a relationship may be formalised by the CSIRT 'adopting' the WARP and working together to provide information and develop skills; if CSIRTs have WARPs within their constituency then such arrangements have particularly clear benefits.




In some cases, CSIRTs may be able to help the WARP community deal with incidents, but experience has shown that incident response works best if there are few steps in the communication chain. There will be fewer opportunities for misunderstandings if the WARP member works directly with the CSIRT once the incident has been reported, rather than via the WARP.

How can they develop?

As a WARP develops its skills and resources it may wish to help its community to remedy incidents as well as preventing them. It may be better to create a separate CSIRT (perhaps shared by a group of WARPs) to do this work, rather than risk changing the WARP's existing relationship with its community. An incident response team that is advertised as an incident handling contact for its community will receive more sensitive information about the members (such as reports of compromised systems from external sources) and will be seen as having more responsibility for them. The resources required by a CSIRT are likely to grow as the number of incidents (or the number of members of the constituency) increases, since each incident will require individual attention. Conversely a WARP should retain much the same workload as its community grows, so long as it maintains a common focus. Once the community gets too large, or too diverse, for a single WARP then additional WARPs should be formed to sustain the level of trust within the communities and possibly achieve economies of scale.

The most effective solution is to combine the two types of operation: using a WARP, or group of WARPs, to reduce the number of incidents through preventive measures, and a CSIRT to handle those incidents that do, nonetheless, occur. Both can work together to share information about the prevalence and severity

of incidents to help member organisations promote and prioritise security measures and response, thereby further reducing the number and impact of security problems.



JANET®, SuperJANET® and UKERNA® are registered trademarks of the Higher Education Funding Councils for England, Scotland and Wales. The JNT Association is the registered user of these trademarks.