The Development of Warning, Advice and Reporting Points (WARPs) in UK National Infrastructure

Tony Proctor

School of Technology, University of Wolverhampton, Wulfruna Street, Wolverhampton, WV1 1LY, UK
t.proctor@wlv.ac.uk

Abstract. This purpose of this paper is to examine the development of Warning, Advice and Reporting Points (WARPs) as part of the information sharing strategy for UK National Infrastructure. It identifies and discusses the origins of the Computer Emergency Response Team (CERT) and Information Exchanges. It then reflects on the authors own experience of managing Warning, Advice and Reporting Points, defining and describing these important forums for information sharing in the UK information security community and beyond. One of the problems in protecting critical infrastructure is how to get the right information to the right people. The paper identifies key drivers for information sharing. It outlines the University of Wolverhampton involvement in the WARP programme since 2006 and the success that has been achieved creating and working with several WARPs in the public sector.

Key words: security information, information sharing.

1 Background

Delivering appropriate information to the right people is an essential aspect of critical infrastructure protection. This is equally applicable in both incident prevention and incident response. Two incidents, sixteen years apart identify the need for improved methods of information sharing.1988 experienced the first major internet incident, the Morris Worm. A report written by Purdue University [1] concludes that, the attack, "*should also point out that we need a better mechanism in place to coordinate information about security flaws and attacks*. *The response to this incident was largely ad hoc, and resulted in both duplication of effort and a failure to disseminate valuable information to sites that needed it" and "methods did not ensure timely, widespread dissemination of useful information".* Sixteen years later, the report into the 9/11 attacks on the US identifies a failure in information sharing. The US Government [2] describes the biggest impediment as, *"the human or systemic resistance to information sharing"*. It describes the use of databases that might not normally be thought of as intelligence (e.g. customs or immigration) providing an *"immense storehouse of information".*

The UK Government describes the sharing of information about the risks facing networks as, "beneficial to both government and industry".

S. Bologna et al. (Eds.): CRITIS 2011, LNCS 6983, pp. 164–174, 2013.
© Springer-Verlag Berlin Heidelberg 2013

It describes mechanisms through which one company can learn from the experiences of others, "without fear of exposing company sensitivities" as being an opportunity for every participant to improve their level of assurance [3].

The increasing availability of electronic information combined with inter-organisational collaboration and sharing of services provide some of the other drivers for information sharing. But there are barriers to overcome in order to develop information security, information sharing.

A WARP is a community based service for sharing timely advice relating to information security threats, incidents and solutions. WARPs were developed by the Centre for the Protection of the National Infrastructure (CPNI) as part of their Information Sharing Strategy. They recognised the need to provide a cost-effective way to facilitate information security among a diverse range of organisations, many of which form part of the critical national infrastructure.

In 2007, the University of Wolverhampton in collaboration with West Midlands Police, created a WARP for Local Government in the region. WARP is a developmental project that has attracted both national and international attention. The challenge is for it to both develop as a concept and adapt to the changing needs of the members during a time of decreasing budgets.

2 The Development of Information Sharing

The report into the incidents of 9/11, supports establishing a culture where availability of information is defined not on a "need to know" but instead on a "need to share" basis. The report makes an interesting contrast between the penalties for over-classification of information (cost to the organisation) and the risk of sharing (criminal, civil and administrative sanctions). It recommends that procedures should provide incentives for sharing. This provides a better balance between "securing" and "sharing" information. It provides weight for this intention, identifying the President as the person to resolve the legal, policy and technical issues in order to create a trusted information network.

From a technological perspective, the report recognises that each organisation operates their own databases. It recommends that "horizontal searching" is available across agency lines and that the security remains protected by the design of the network and Information Rights Management (IRM).

In the UK, the demand for information sharing across the public sector continues to grow. In the Local Government Sector there is a requirement to share information with the health service, police and others. Some of the challenges that this presents are illustrated by Leicestershire County Council [4] who define an information sharing protocol for multiple partners. This helps to address one of the main issues affecting organisations who need to share information; establishing the rules for sharing.

2.1 The Emergence of the Computer Emergency Response Team (CERT)

The Morris Worm was created by Robert Morris, a student at Cornell University. In the Perdue University Report (described in section 1) it is stated that, "It is clear from

the code that the worm was deliberately designed to do two things: infect as many machines as possible, and be difficult to track and stop. There can be no question that this was in any way an accident".

Developed for DEC hardware supporting the UNIX operating system, the replication of the Worm caused a denial of service to approximately 6 000 machines. This accounted for more than 10% of the internet at that time. The code allowed the Worm to replicate multiple instances on a single computer, resulting in a denial of service. The cost of the damage exceeded $10 million. Morris received a community service sentence and a 3 year probation order. It is interesting to consider what the penalty would be today for creating a 10% denial of service on the internet?

The US Government determined that a response was necessary in order to address future problems. In 1989 the first CERT (CERTCC – CERT Coordination Centre) was established in partnership with Carnegie Mellon University [5]. Other nations followed suit. In 1992 the UK Government created the Unified Incident Reporting and Alert Scheme (UNIRAS) [6]. The functions of this were to respond to electronic attack and other significant IT security incidents, warn about IT security incidents and vulnerabilities and to gather information relating to IT security incidents.

Today, the UK National "CERT" is formed by two organisations. GovCERTUK is operated by the Government Communications Headquarters (GCHQ). Essentially, GCHQ has overall responsibility for the .gov.uk domain and anything attached to it. The other organization which helps to provide a national CERT function is CSIRTUK, operated by CPNI (see 2.2). In addition to these national "CERTs", the Cyber Security Strategy of the United Kingdom [7] announced the creation of the Office of Cybersecurity (OCS) and Cyber Security Operations Centre (CSOC). The OCS provides strategic direction on cyber security and information assurance for the UK and works with private sector partners on exchanging information and promoting best practice. CSOC's primary role is to actively monitor and coordinate incident response. The key differentiator in role appears to be that one is "Strategic" and the other "Operational".

Fig. 1. Word Map of Computer Incident Response Teams (CERTs and CSIRT FIRST Members) FIRST [8]

The darker areas in Figure 1 identify many of the nations that operate CERTs and / or CSIRTs. CERTs and CSIRTs perform a similar role, discussed by GovCERT.NL [9]. US-CERT [5] describe themselves as, "providing response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with state and local government, industry and international partners". WARPs have been compared to the "outreach component" of a CERT [10].

2.2 Centre for the Protection of the National Infrastructure (CPNI)

In 1999 the UK established the National Infrastructure Security Coordination Centre (NISCC). More recently renamed the Centre for the Protection of the National Infrastructure (CPNI), it is the UK Government body responsible for providing security advice to the businesses and organisations which make up the national infrastructure. They are the Communications, Emergency Services, Energy, Finance, Food, Government, Health, Transport and Water sectors [16]. CPNI's focus is primarily to defend against attacks from terrorist or other sources of an electronic, physical or personnel security nature.

2.3 Information Exchanges

As part of an information sharing strategy, CPNI operates Information Exchanges (IE). They are defined as, "a mechanism through which one company can learn from the experiences, mistakes, and successes of another, without fear of exposing company sensitivities" CPNI [3]. An Information Exchange is based upon the personal trust of representatives, sharing information in a confidential meeting. Representatives at Information Exchanges are expected to attend all meetings, which are held every two months. Meeting face-to-face is intended to build up a small, trusted community with a common interest. It is considered that strangers may inhibit the sharing of sensitive information. So each organisation is permitted a maximum of two representatives and substitutes cannot attend. At the time of writing, there are 12 information exchanges as shown in table 1.

Table 1. The 12 Sectors for which CPNI Operates Information Exchanges

Aerospace and Defence Manufacturers	Financial Services
Communications Industry	Managed Service Providers
Personnel	Northern Ireland
Pharmaceutical Industry	Network Security
Supervisory Control and Data Acquisition (SCADA – critical infrastructure and Control Systems)	European SCADA

2.4 WARP

A WARP or Warning, Advice and Reporting Point to cite its fullest definition, is a community based service for sharing up-to-date advice on information security threats, incidents and solutions. WARPs were developed by NISCC. They now form part of CPNI's Information Sharing Strategy. CPNI states that, "A WARP works because its membership is a community, based on geography, technology, business need or another area of common interest, CPNI [11]. On the ground, this means that a security concern of one member is probably a concern of the other members and their WARP is the most effective way of sharing information between them".

WARPs are an extension to the Information Exchange concept. They have fewer rules, can operate beyond the critical infrastructure sector and are independent (as they are not directly operated by CPNI). A WARP provides warnings, advice and is a place to which incidents may be reported. Warnings are most commonly distributed via email and are filtered, hence WARP members receive only relevant information. Advice is facilitated via a number of methods: directly from the WARP Operator, regular face to face member meetings, member to member discussions and a virtual network of experts that has been established. Table 2 summarises the processes that provide WARP functionality. WARPs have developed an appropriate structure for the dissemination of information: they can create links with their peers, share information with other WARPs and other relevant organisations (e.g. GovCERT, CPNI, and Ministry of Defence) nationally via the WARP Operators Forum.

Table 2. WARP Function and Process

WARP Function	Process
Warnings	Daily issue of warnings, advisories and news via email (SMS, RSS and telephone may also be used)
Advice	Available via email and telephone. Self-help advice is facilitated by discussion in regular face to face meetings
Reporting Point	Incidents are discussed in the regular meetings. Members may also report incidents via email or telephone

3 The University of Wolverhampton as a WARP Operator

Following a WARP presentation delivered by NISCC, West Midlands Police approached the University of Wolverhampton with a view to creating a WARP for the West Midlands region. This partnership was joined by the Local Government Association for the region.

Initial funding was provided by the Higher Education Innovation Fund (HEIF) and the Office of the Deputy Prime-Minister (who created a fund to develop WARP in the Local Government sector). The first WARP established by the University was specifically for the Local Government community in the West Midlands region of the UK. West Midlands Councils WARP was officially launched by the e-Government Minister at the end of 2006. Reference to "UoW WARP" in the remainder of this paper relates to all WARPS operated by the University of Wolverhampton.

3.1 West Midlands Councils WARP (WMCWARP)

Initial activity was focused to identify the resources and technical infrastructure essential in order to successfully operate a WARP. Membership of the WARP was offered as a six month free-trial. Following slow uptake, this was extended to twelve months. The WARP then became a subscription service. At the end of 2008 there were 11 subscribing members. At the time of writing, WMCWARP has 26 council members from a possible constituency of 33 Local Councils in the region.

3.2 East Midlands Government WARP (EMGWARP)

The East Midlands Government WARP was founded in 2006. This WARP was established as a partnership between the Local Government Association for the region, Leicester City Council and Mid-Yorkshire Chamber of Commerce (MYCCI). In 2007, MYCCI ceased involvement with WARP. Since this time, the University of Wolverhampton has been contracted to provide warnings and alerts for the EMGWARP. At the time of writing, EMGWARP has 29 council members from a possible constituency of 46 Local Councils in the region.

3.3 South East Government WARP (SEGWARP)

In 2009, the organisation responsible for supporting the activity of Local Government in the South East of England, South East Employers (SEE) decided to create a WARP. SEE contracted with the University of Wolverhampton as an experienced WARP Operator. SEGWARP achieved early rapid growth, recruiting over 20 subscribing members during the first six months. These remain the core members. At the time of writing, this WARP has 25 members.

3.4 National Health Service WARP (NHSWARP)

The NHSWARP commenced in 2008 as a pilot programme for NHS organisations, initially for the West Midlands region. Six members were involved in the pilot stage, half of whom became paying members. This WARP has not achieved the same level of maturity compared to the other WARPs operated by the University. The primary reason for this is the absence of available funding. However, developments have been closely monitored by information assurance leaders in the Department of Health. And the NHSWARP has attracted interest from the private health sector.

Consideration may therefore be given to changing the focus from a WARP that is for the NHS alone to an inclusive Health-Sector WARP. US-CERT has expressed an interest in this WARP.

4 WARP Resource Requirements

It is not a pre-requisite for a WARP to operate an automated system. However, the Author's experience suggests that it is both necessary and practical to create a professional WARP. The essential requirements of this system are; creation of user accounts and preferences, creation of alerts, filtering of alerts and issuing alerts. The system needs to be accessible by members from multiple locations. Hence a web based service is highly desirable.

Most WARPs use the Filtered Warning Application (FWA). This was originally developed at Microsoft, with licensing and intellectual property belonging to CPNI. The FWA has undergone a number of revisions and security assessment.

Different staffing models are operated by different WARPs in order to administer the system and issue alerts. The Wolverhampton model is primarily based on an academic member of staff supported by a Technical Assistant. Security is observed in recruitment process by ensuring that references are sought and this is supplemented by a Criminal Records Bureau (CRB) check.

5 Identifying Security Issues and Trends

This section summarises the main issues discussed within the WARP membership since 2007. The majority of the "Advice" and "Reporting" aspects of WARP are currently achieved via regular closed meetings. For UoW WARPs, these meetings occur quarterly. Each meeting operates a standard format with an agenda and minutes. The agenda includes a roundtable where members advise the group on any incidents that have occurred and how they have been addressed. It is also an opportunity for the participants to discuss their current work and provide feedback on the WARP itself. Each meeting includes a guest presentation. They will be from an expert speaker. The topic will be something of particular interest to the members, chosen by them. It will be an "agnostic" presentation: discussion of specific products or services is not allowed. The presenter is not allowed to attend for any other agenda items unless requested by the members.

There do not appear to be any difficulties in encouraging members to share information. The greater difficulty is achieving participation in meetings by the wider membership. Those who do attend a meeting will usually re-attend. However, there are members who do not attend meetings. Hence the maximum attendance at meetings is typically half of the membership.

The majority of problems reported by WARP members relate to the accidental loss of data. Typically this involves usb memory sticks, smart phones and laptops. Awareness in tackling this problem has increased. Most reports now state that devices were encrypted, whereas in the past this was not the case. Another trend (which has been encouraged through WARP) is the reporting of incidents to the Information Commissioners Office (ICO). Again, this is now more routine than exceptional.

The ICO have presented at a number of WARP forums with the intention of developing a relationship with WARPs in order to ensure that the most productive actions are taken in the event of a data loss.

Staff related issues are also common. These may range from reports of staff storing sound and video files on work based storage, through to the storage of pornographic material and harassment via email.

Compliance is another aspect of importance since the WARP began in 2007. The main requirement in Local Government has been the Code of Connection (CoCo). This requires the implementation of a detailed set of controls in order to connect to the Government Secure Extranet (GSx). It is necessary for Councils to do this in order to share information with Her Majesty's Revenue and Customs (HMRC). The current focus is moving towards the Public Sector Network (PSN). This aims to provide secure networks to a private cloud in which the public sector can operate. PSN has a separate code of connection.

2011 has experienced significant reductions in public sector funding. For some councils this has resulted in a loss of staff across all areas including IT. There is also an increase in the sharing of services. This for example, may involve one IT Department providing services for two or more councils. The other trend which has implications for security is the increased involvement of the private sector in public business. Contracting out IT Departments means for some councils that their whole IT function is provided by a private sector company. All of these issues have a potential impact for WARPs. Budget reduction could threaten the sustainability of the programme, sharing IT services may introduce a desire to share the WARP subscription and an outsourcing company may not wish to be a member of a local government WARP.

Many of the issues discussed by WARP members have related to the requirements of the CoCo. Hence some of the key requirements that members have needed to address include: the need for classification of data, securing remote access, penetration testing and log management. In more recent discussions, the use of Social Networks has been identified as an issue. The key conclusion from these discussions identified the necessity for each organisation to have a social network usage policy.

6 Other WARP Initiatives

Uow WARP has been involved in a number of trials and has provided alerts to other organisations via peer to peer links. These organisations have included the London WARP and the Law Society. UoW WARP has furthermore, engaged in activities to promote information assurance in the smaller business sector.

6.1 "Olympic WARP"

In 2008, the author engaged in the development of the WARP concept to support the 2012 Olympic Games. The intention was to strengthen information assurance for the games through the provision of a facility for security information sharing involving all parties rather than the main contractors alone. Whilst ddiscussions have taken place with several key stakeholders, it has not been possible to find a sponsor for a WARP initiative to support the 2012 Games.

6.2 International WARPs

The WARP programme is a UK initiative. However, it has attracted considerable interest from overseas. In 2007 employees of the electronics giant Hitachi visited the University of Wolverhampton. Following this, a decision was taken to create a WARP for the Hitachi Corporation's internal operations. A WARP has been created in the Irish Republic in lieu of a national CERT and in South Africa, the University of Johannesburg have created a WARP. More recently, a WARP has been registered for Flemish ICT Companies in Belgium [12].

In addition to these formally registered WARPs there has also been considerable interest from other countries. In Holland, there was a project to examine the use of WARPs with schools. More recently interest was expressed from a Chinese organisation. Overseas WARPs raise some interesting questions; how much should international WARPs be promoted / encouraged and what information (if any) should be shared with them? It is also necessary to consider how engaging with foreign organisations may affect the involvement of UK Government with WARP (e.g. CSIRTUK, GovCERTUK).

7 European Information Sharing Initiatives

An EU funded programme has been undertaken to address critical infrastructure protection through information sharing. The National & European Information Sharing & Alerting System (NEISAS) is an EU funded project created in 2009 to enhance critical infrastructure protection through trusted sharing of information [13]. Some initial findings of the project identify the need to provide a "true" exchange of information rather than simply a "push" web portal, enable the owner of the information to choose who can read it, support 'peer to peer' exchange between national platforms (with no central system) and enforce the Traffic Light Protocol (TLP) [14] for compliance for distribution.

NEISAS identifies key definitions and describes the community within which information sharing takes place as a "Trust Circle" which is facilitated by a "Trust Master". It provides a good example of how a member of a trust circle can share sensitive information without damaging reputation (i.e. the member discusses the issue with the trust master who then raises the issue without reference to that individual member). In developing a prototype application for cross-border information sharing, it has also defined some of the key requirements for such a system. One of the main challenges for this is overcoming the problem of losing control of distribution once an email has been sent. NEISAS suggests overcomes this by implementing Information Rights Management .

Another EU-funded project is the Framework for Information Sharing and Alerting (fisha).This aims to improve the security awareness amongst home users and smaller businesses by the creation of a European information sharing and alerting system [15]. The partners in this project are CERT Polska, CERT-Hungary and the University of Gelsenkirchen.

8 Conclusions

The techniques and concepts related to information security emerge from a highly secure world of secrecy. For example, cryptography was largely an application exclusive to the military and security services less than 20 years ago. The incredible growth of the internet and the rapid pace at which both internet applications and hacking techniques have developed, has made it necessary for these techniques and concepts to be applied increasingly in general use. Along with this has been the development of ways to share information across the public and private sector in response to increasing globalisation and the use of technology. This places a requirement for an environment where "secrecy" is counter-productive but where openness needs to be achieved in a "managed" way (because no one wishes to declare their vulnerabilities to a potential attacker or to be the subject of negative publicity due to the disclosure of an incident). The technical solutions to security issues have existed for some time and continue to be developed in order to meet changing requirements. However, they can only provide partial success because of a lack of effective information sharing and awareness.

The findings of this work suggest that information sharing systems for information security are still in their infancy. National CERTs have spread around the world (although there remain many countries where they remain absent e.g. many countries in Africa). They are largely, closed organisations often operated by the security agencies of their respective countries. In working largely independently, WARPs are able to achieve a more advanced level of information sharing with their communities. However, they do require development in order to fully achieve their goals. strategy. The NEISAS project has addressed some of the main issues for information sharing and show how they can be built into a software application.

UoW WARP sources the vast majority of information from vendors and independent review sites and evidence suggests that this is common for the information security community as a whole. For a national CERT to be effective in protecting their online citizens it is necessary for an ongoing dialog with organisations such as WARPs. Sharing information in order to improve security is still perhaps a difficult concept for some. It is evident that there is a great opportunity for a range of activity in this area and a requirement for greater openness in order for all to benefit from the knowledge and experience that exists.

References

1. Spafford, E.H.: Purdue Technical Report CSD-TR-823. The Internet Worm Program: An Analysis. Illinois: Purdue University, Department of Computer Sciences (1999), http://spaf.cerias.purdue.edu/tech-reps/823.pdf (accessed: March 29, 2011)
2. U.S. Government: The 9/11 Commission Report, 416 p. WW Norton & Co. (August 2004), http://govinfo.library.unt.edu/911/report/911Report.pdf (accessed: March 29, 2011)
3. CPNI, Who we work with, Information Exchanges (2011), http://www.cpni.gov.uk/about/who-we-work-with/information-exchanges/ (accessed: March 29, 2011)

4. Leicestershire County Council, Information Sharing Protocol (2009), http://www.leics.gov.uk/information_sharing_protocol.pdf (accessed March 29, 2011)
5. US-CERT, About Us (2010), http://www.us-cert.gov/aboutus.html (accessed March 29, 2011)
6. UNIRAS, Unified Incident Reporting and Alert Scheme (2006), http://web.archive.org/web/20010418174646/http://www.uniras.gov.uk/ (accessed January 01, 2011)
7. Cyber Security Strategy of the United Kingdom (Cm 7642). TSO, London (2009), http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf (accessed February 11, 2011)
8. FIRST, First Members (2010), http://www.first.org/members/map/ (accessed February 11, 2011)
9. GOVCERT.NL, SETTING UP A CSIRT (2005), http://www.govcert.nl/render.html?it=86 (accessed January 08, 2011)
10. Proctor, T.: WARP speed ahead (2008), http://www.bcs.org/server.php?show=ConWebDoc.18595 (accessed March 30, 2011)
11. CPNI, Information sharing concept (2010), http://www.cpni.gov.uk/ProtectingYourAssets/informationSharing.aspx (accessed January 08, 2011)
12. WARP 2011, Warp Directory (2011), http://www.warp.gov.uk/directory.html (accessed March 30, 2011)
13. NEISAS 2011 (2011), https://www.neisas.eu/ (accessed March 28, 2011)
14. New Zealand Centre for Critical Infrastructure Protection (CCIP) 2011, Home, Incidents, TLP (2011), http://www.ccip.govt.nz/incidents/tlp.html (accessed March 28, 2011)
15. fisha 2011, The Project (2011), http://www.fisha-project.eu/the-project (accessed March 28, 2011)
16. CPNI, About CPNI (2011), http://www.cpni.gov.uk/about/cni/ (accessed July 22, 2011)