

WARPS CASE STUDY

MID-YORKSHIRE CHAMBER MYCCI: TELECOMS HIGH-RATED WARNING

On the morning of the 4 October, Jim Sunderland, Information Security Manager and MYSWARP Operator for Mid Yorkshire, sent out a high-rated telecommunications warning to all members following a set of bogus telephone calls to their sites. The caller had asked for a member of staff by name, and then informed them that they were calling from the organisation's telephone service provider.



The bogus caller then requested that they dial 07 (or in some instances 05) prefixed number, so that a line test can be completed overnight. This resulted in the subscriber receiving a substantial bill.

The Discovery:



Company A had discovered an unusually high telephone bill. An internal investigation revealed that a call had been received, purporting to come from their telecoms contractor, asking the member of staff to dial a 07 prefixed number and leave the line open overnight to enable some testing to be completed.

The caller not only identified themselves as calling from the telecoms contractor, but asked for a member of staff by name, which means that either the telecoms contractor or Company A had had their records penetrated, or that someone with insider knowledge was involved.

When Company A discovered the charge on their bill they contacted Company B, their telecoms contractor (and a member of MYSWARP). Company B immediately confirmed the details of the incident with Company A, and then issued a specific warning to their customers, complete with contact details in case any of them should suffer, or had suffered, a similar incident.

WARP case study MYCCI V 1.1 December 2006

Company B provided the MYSWARP Operator with full details of the incident and an anonymised warning was prepared and circulated.

The Process:

Jim's role as a WARP Operator is to identify any such incidents and to report them to his WARP members as quickly as possible. He explains: "My daily task is to trawl several information sources such as news items, incoming emails, the WARP bulletin board, the CERTs forums, virus warnings and specialist sites for local government software. If there is any pertinent information, I circulate it to the members who have signed up to the service. However, as regards this incident, I also rely on information sent to me by members, who feel that their systems have been otherwise compromised or breached."

The Trust Factor:

Most of Jim's warning incidents are usually software related although the WARP member service also covers Telecoms and Convergent Technologies. Jim explains: "We have relatively few telecom warnings but when we do, we also have to make sure they aren't a hoax."

In this instance, Jim felt comfortable with the fact that the warning could be anonymised and that there was a trust factor with the telecoms provider who help him gather the necessary information. In addition, he was told (by the provider) that they had already talked to all their customers to warn them of the infringement.

Since the incident there have been no further reported instances, but as the incident was only discovered because someone applied due care and attention to the processing of the telephone account, it may be that there have been similar 'attacks' which have gone unnoticed. Jim concludes: "It is vital that all members regularly check and analyse any anomalies in their day-to-day activities because it is only then that we, as a trusted network, can work together effectively and eliminate these kinds of attacks."

