The ethics of disclosure:

Over the last two weeks, the IT world has been looking on in fascination as giants of the network and security have been locked in courtroom battles in the United States with an individual and a conference organiser.

It all started when Cisco became aware of the proposed content of a presentation being prepared by an employee of Internet Security Systems, Michael Lynn. This presentation was to have been presented at the Black Hat conference in Las Vegas. This is one of the leading security conferences of the year where many hackers as well as security companies attend presentations.

Michael had been working on a software vulnerability, and an exploit, for a number of months on Cisco networking equipment. Internet Security Systems and Cisco had been working together to develop a fix for the vulnerability, and planning a public release of information when the fix was made available.

It appears that Michael became frustrated with the way that Cisco and Internet Security Systems were handling the publication of this vulnerability, and decided to take action himself.

When Internet Security Systems heard about this, they immediately moved to distance themselves from Michael, and he resigned from the company. They then informed Cisco that this information was going to be made public, and that Cisco may want to take some action.

Cisco went to court, and was granted a temporary restraining order against both Michael and the conference organisers. Personnel from Cisco were then engaged in the removal of pages from the pre-printed material for the conference, and Michael agreed to deliver a different presentation. They have also sued Michael for illegally disclosing proprietary information.

However, there are now hundreds of web sites around the world that are making various versions of this presentation available for download. Some of them even have the original Internet Security Systems logos and standard presentation templates on them.

What was in this presentation that could have caused these giants to react so quickly and with such gravity? Michael had identified a method of attacking Cisco devices that reportedly carry 60% of the Internet traffic and taking control of these devices. This possibility was described by Michael as being an “Internet Pearl Harbour”. Once control had been taken of all these devices, the potential for disaster was huge. The most basic, and devastating, attack would be to disable their functionally as Internet routers, effectively destroying the Internet. Other, more complex, attacks could have resulted in malicious users gaining unauthorised access to data and networks. The patch from Cisco to fix this vulnerability would normally be distributed via the Internet, but with that unavailable, it would take an extremely long time to get systems back and secure.

The detail of how to carry out this exploit was contained in the presentation. While it did not contain every step needed, it is apparent that a knowledgeable person would have enough information to create the exploit.

This episode, that Michael joked could end up with him being confined to Guantánamo Bay, has again sparked the debate about the ethics of vulnerability disclosure to the public. Some sections of the debate are pushing for an agreed time period from vulnerability discovery and vendor notification to publication. This time frame varies, and is to provide the vendor with sufficient time to develop a patch, test it, and make it publicly available.

There have been a number of vulnerabilities disclosed recently that manufacturers have not had time to issue patches for and these are considered by many in the security to be of particular concern.

Developers are getting exploits to these vulnerabilities into the wild more quickly than ever before, and they can be extremely hard to defend against.

Hopefully, incidents like those with Cisco will focus people's minds on getting patches issued before the vulnerabilities are made public, thereby reducing the likelihood of an attack being successful. There is also a responsibility on the part of technology users as well as technology manufacturers to get the issued patches installed in a timely manner.