What has 2006 got in store for us?

We have had a pretty busy year in 2005 in the Information Security arena.

In the past year, we have seen some staggering increases in the volume of unsolicited email (SPAM) and malicious code (MalWare).

The security research firm iDefense published statistics that show that more then 6,000 new keystroke loggers were released into the wild and sent to unsuspecting Internet users. This was an increase from approximately 3,000 in 2004. These keystroke loggers, when installed, will record every keyboard entry made by any user on that PC. That means that credit card numbers on retail sites, online-banking authentication credentials, that saucy email to a co-worker etc are all being recorded and sent back to the hacker for analysis. Typically, the author of this MalWare is looking for financially exploitable details such as credit card numbers, online-banking credentials and software license codes. In some ways you almost have to admire the ingenuity of some of these guys. To make life easier for themselves, they have started writing analysis routines into the loggers that will weed out the credit card numbers and passwords, and only send those to the hacker, making his job that much easier!

These keystroke loggers and other Phishing (and Spear Phishing) techniques have led to a huge increase in the area of Identity Theft. In the United States, more than half of all complaints to the Federal Trade Commission were related to Identity Theft. The FBI estimated that computer related crime in the US was responsible for losses of more than $67Billion in 2005. A significant portion of this figure is based on Identity Theft. In most areas of Information Technology, Europe, and particularly Ireland has been 12-18 months behind the US. We are seeing rapid increases in the number of Identity Theft frauds being committed, and this will continue to increase.

Many of these crimes are actually committed using information gathered in the Offline world through actions such as dumpster diving and letter box theft. This will continue, but the online theft will increase in the near term. Many organisations such as banks are reviewing their methods for customer identification and authentication given the threats, particularly form Phishing. In the last months, we have seen AIB develop a code-card and also RaboDirect deploy a one-time passcode generator, Digipass. These are well proven methods to thwart the Phishing attempts at credential theft.

But what does 2006 have in store for us?

We have already seen what is known in the security industry as a Zero Day Exploit. This is where information on a security weakness, in this case on Microsoft Windows, is made public before the manufacturer has completed the patch to address the vulnerability and make it available for users to apply. As a result of this information disclosure, many thousands of systems worldwide were infected with malicious code that exploited the vulnerability. Microsoft did take the unprecedented step of releasing a specific patch for this vulnerability outside of its normal monthly patch release procedure. However, the release of the information by the organisation that discovered the issue before a fix was available is considered by many in the Information Security world as unethical, and very dangerous. There is a feeling at the moment that 2006 may be the year of the Zero Day Exploit. In the last couple of

weeks, Oracle was the target of another disclosure. At the Black Hat Federal Conference in Washington at the end of January, a researcher disclosed a Zero Day Vulnerability on the Oracle web suite. An organisation like Oracle that runs a media campaign based on their database suites being “Unbreakable” from a security perspective will always attract this sort of attention.

We are also going to see more organisation with Internet based applications such as retailers and financial institutions suffer from application based hacking, not just the common attacks on un-patched servers that we have been seeing over the last couple of years. This is where weaknesses in the design and implementation of the application layer are exploited to gain unauthorised access to the services, or to gain access to another customer’s information when logged on. People are starting to get the message regarding the timely installation of patches and bug fixes from vendors and the hacking community are therefore moving on to the next layer to attack.

In 2006, the thorny issue of digital rights abuse will raise its head again. In 2005, IRMA went to court to take a civil case against 17 individuals that they believed had infringed the copyright of recording artists. These actions were based on data provided of alleged serial file sharers from a US organisation known as Media Sentry. Many of these cases were settled with the payment of a fine, but some are still being pursued. In the last weeks, IRMA has again been in the courts, this time they secured the identification of 50 alleged file sharers from the Internet Service Providers based in Ireland. With this information, IRMA will again bring civil cases against those identified. The threshold on this occasion was anyone that had uploaded/downloaded more than 500 songs. Identification of a company by the ISP in question could be very damaging for that company. The organisation may not even be aware that some of the staff were breaking the Copyright Act, and they could find themselves in court, and published.

Lastly, 2006 will be the year where compliance and certification with standards such as the IS17799 will really take off. In 2004 and 2005, a handful of companies became certified, but we are already seeing the competitive advantage that such a certification can bring. It is a key part in many organisations such as data centres winning tenders in the face of international competition.

Finally, as with all predictions for the year ahead, the only thing that we can be certain of in Information Security is that something will come along and blindside you at 4pm on an idle Tuesday afternoon (the Sunscreen song from Baz Luhrmann).