New Year Resolutions: Computer Security
by Calum Macleod - Senior IT Consultant at Cyber-Ark -
Monday, 27 December 2004.

It's that time of the year again when we all reflect on the year gone by and consider what lies ahead.

In the world of IT, most of us have been grateful onlookers when we consider the misfortunes of others, and wonder how they could be so irresponsible as to allow such mishaps, or more likely thank our lucky stars that yet again we've escaped, and hopefully no one above us asks too many questions about how we would have dealt with a similar situation. So as we consider our resolutions work-wise, it might be good to reflect on some of the twists of fate suffered by some of our colleagues over the past year, and try to learn from someone else's bitter experience.

March saw a well known bank having to pay a substantial fine for failure to produce some old emails on time, although they were not alone in this since a number of other companies who fell under the Sarbanes-Oxley umbrella suffered similar fates. Under the act, public companies are required to archive any and all financial data, and also to keep a record of a document's lifecycle, including who within the company had access to, viewed or amended a given document. The information also needs to be retrievable in just two business days!

August was the month for leaks! Not that kind – well maybe it was given the summer we had. People had nothing better to do it seemed, or maybe it was just a bad month for news, but suddenly it was raining source-code. First it was id Software, and then later in the year it was Microsoft, and lately Valve got hit. What is difficult to understand is why anyone who should not have access would even know where to look. Come on folks, we're talking about a couple of hours work to make sure that the stuff is so out of sight that not even Santa would find the "grotto"! August continued to be a bad month for consumer confidence with the news that Hotmail had some flaws that allowed access to other peoples email.

October brought the issue of using home computers for work to the forefront, well in the Netherlands at least. Known as the Tonino affair, it involved case of Dutch public prosecutor putting his personal PC on the street with the garbage, believing it was defective due to a virus. A taxi-driver who happened to be passing by, saw it, and took it home with him. He easily got it to work and took it to a journalist. The hard drive contained information on high profile cases, and the system also allowed access into all of Tonino's email traffic. Adding insult to injury, hackers raided Tonino's email box and placed important correspondence on the Internet. Suffice it to say the unfortunate gentleman's caseload is not what it was!

So how are you working from home? – Using your private PC, and downloading confidential information from the office, and only with the best of intentions – to make your life easier and to be more productive for the company? Unfortunately it seems that many of those PCs leaving the store may not be as safe as we'd like to think since frequently they haven't been patched with the latest and greatest security fixes, which leaves them, open to all kinds of nasty stuff. And then off we go providing easy remote access with all kinds of whizzbang VPN stuff, and allowing colleagues to download all kinds of confidential data.

Christmas comes along and if you're lucky maybe the employee from Human Resources threw the old PC in the bin. It might be worse – they may have given it to the kids!!

December saw yet another Government minister fall prey to the wonders of email. Email is a great invention, I simply can't imagine life without it, but I believe that frequently we forget that "the keyboard is mightier than the sword", because it has this nasty habit of biting from time to time. Mind you our public servants continue to seemingly totally miss the point. Using email is not intended to be used by politicians as a means to demonstrate to the rest of us that they are IT literate! Mind you it seems that government has found the answer – Whole scale deletion of mail is the latest Whitehall brainwave. Not only could you or I end up as a guest of HM for doing something similar but it seems they still haven't quite got the point. They'll probably delete them before they send them for security reasons!

So there we have it, a year of unfortunate mishaps, and many more besides that. But how do you avoid being next year's talk of the town...

Well maybe a few resolutions would help:

1. I resolve to put in place security layers such as File Access Control and Version Control according to our company's policy so that only authorized users will be able to delete or modify documents.

2. I resolve to implement monitoring and auditing features to insure that all activities are logged, and that reports can be issued and sent according to a notification process.

3. I resolve to put controls in place to ensure that users cannot copy confidential information to unauthorised systems.

This would be at the very least a start, but in the event that you find this all too much trouble, and you think that this kind of stuff only happens to other people.

4. I resolve to look into a good personal liability insurance policy… because the chances are I might need it.