

Information Risk - It's not just viruses

By David Biggins

The information risk that people see most often is represented by a stream of virus and vulnerability alerts – during March, new viruses in just two families were appearing at the rate of more than one per day. Worryingly, it is now normal for new viruses to create remote control “back doors” into the computers they infect. These allow the virus authors to take over victim computers, to harvest personal information such as electronic banking details from them, to use them as relays to attack corporate systems or to use them to disseminate spam/junk mail anonymously. Recent reports show a worrying trend of organisation between spammers, virus writers and organised crime.

However, these are known and relatively static problems, with long-established (if imperfect) technical defences and known management solutions. They should represent the smallest part of Information Risk, and only remain an on-going problem because of three factors. One is undoubtedly the number of vulnerabilities in Microsoft products, allowing attacks to succeed so often. It must, however, be admitted that there are also vulnerabilities in products such as Linux, and independent reviews have shown little difference in code quality between Microsoft and open source products. The second is the effective global monoculture that allows attacks on Microsoft products to succeed so widely. The key factor, however, is almost certainly human nature – the major vulnerability will always be the users of any information system. As with a car, you can design and build as much safety into it as you want, but it only takes one loose nut behind the wheel to cause an accident.

Many users fail to take even basic precautions – evidenced by the fact that the “league tables” of infections normally show that the most widespread viruses have typically been in the wild for many months and are often more than a year old. If every computer user had a firewall and an anti-virus package, and kept their system up to date, viruses would soon cease to be such a significant problem. Sadly, I have met many users who installed anti-virus solutions but never accepted the updates, or who disabled the firewall when it interfered with their visit to a single website. Nor is this problem limited to home PC users. A recent survey showed that 40% of companies had not updated their anti-virus software in the previous month. Even if people just did not open attachments claiming to be pictures of Britney Spears nude, or other obviously false claims, the problem would rapidly diminish. Clearly, the problem is that many people are not prepared to accept even minimal restrictions in how they use their PC, in exchange for a gain in security.

The other human problem for information risk is the widespread perception – even among senior management – that viruses and technical vulnerabilities are what information risk is all about. Approach most organisations, and try to discuss information risk, and they will tell you, “Oh, our IT department handles all that – they’ve put a firewall and anti-virus in, so we’re covered”. Sadly, that is nearly the limit of many organisations’ technical precautions – at least until after their first



major incident, after which they get specialists to advise them on the other technical measures that may be required.

Information risk, however, is not just a technical issue, or even just a computing and IT issue. Handling a few technical vulnerabilities can never be enough to protect an organisation properly. If an information risk policy is to be at all effective, it must cover every aspect of a company's operation, from senior management policy to the process of recruiting even junior staff. Sensibly, this fact is widely covered by BS7799 and ISO 17799 – the standards that cover information risk. Unfortunately, only a minority of companies and organisations have an information risk policy at all, and even fewer have even considered implementing a proper risk policy to these standards.

Homeland insecurity

In the USA, the Department of Homeland Security (DHS) was set up following the September 11th attacks. One of its responsibilities is protection of the country's IT infrastructure from terrorist attack; another is the improvement of IT systems to support the fight against terrorists. Yet, the DHS has drawn criticism from the General Audit Office, which claims that the department and its IT infrastructure are at high risk of failure.

Moreover, its deputy CIO (Chief Information Officer) has just this week resigned, having been on paid leave since last June. Her degrees in IT have been found to be from a non-accredited and unlicensed university, calling their value into doubt. It is now also clear that at her previous post, as deputy CIO at the US Department of Labor, it was known that there were issues about her credentials and yet no action was taken – even when she moved to the highly sensitive post at Homeland Security. The US magazine "Government Computer News" has turned up dozens of names of people listing such degrees on their resumes. Prior to that, as White House Webmaster she was accused of threatening contractors with jail if they disclosed the disappearance of White House emails subject to a subpoena related to the Clinton/Lewinsky affair.

This is an information risk failure on many levels. For the DHS's systems to be at risk of failing to deliver their intended function is clearly a major problem. Most people would also take issue with the concept of the risk policy for such a department being determined by someone whose qualifications come from questionable sources regardless of their experience (or by someone who thinks that blanket secrecy is the appropriate response to a problem, during an active Congressional investigation, in a country that has a Freedom Of Information Act). Yet her replacement alone cannot solve the problem. Clearly, there had been a failure to assess her placement properly, both at the Department of Homeland security, and at the Department of Labor.

Fire down below

I am sure that shortly we will all hear stories in the IT press about companies whose systems have failed as a result of the recent underground fire in Manchester. This fire has reportedly left 130,000 homes and businesses without communications. Emergency services are justifiably proud of the fact that their backup plan has left them able to continue to receive 999 calls – but since the tunnels also carry inter-cell cables for some of the mobile companies, it is not at all clear how badly the public's ability to place such calls has been affected.

Remember, too, that this is for many companies one of the busiest weeks of the year, as they push to meet financial year-end targets. Already I have heard reports of one company whose outlying branch systems, instead of failing completely as they were cut off from the main IT site, merely produced the most dangerous results of all – apparently plausible, but wrong. Make no mistake, companies will go under, people will lose jobs and yes, some lives will be wrecked because of this failure.

Privacy and priorities

In the UK and Europe, privacy of personal information is regarded as a civil right, enforced by Data Protection legislation and backed up with standards (notably BS7799 and ISO17799) that assume that such privacy is a key objective, and that compromising privacy is a key risk that must be protected against.

Not all countries have such a viewpoint however and even where the country does, companies and organisations are often slow to regard privacy as a core objective. This is perhaps why investment in privacy protection by corporates is falling behind spending in other corporate compliance requirements, such as environmental programmes.

The human factor

In all of this, the human response is the biggest problem.

- People will not take sensible precautions at even the basic level, unless pressed to do so, or until they suffer some incident such as a major virus attack – and sometimes not even then.
- People will not imagine the concept of large-scale failure and plan for it.
- People will not consider information risk to go beyond the scope of the IT department, nor will they look at the way it impacts entire organisations.

The last of these is the key – until organisations regard the management of the widest aspects of information risk as a core part of their corporate governance, information risk will be stuck as a never-ending fire-fighting operation by the IT department, rather than as something that engages the entire company into understanding the risks, and contributing to their management.

It can't go on

The UK is seen as lagging behind Europe in Information Security, but it has to be said that Information Risk is lagging behind the larger corporate perception of risk worldwide.

Although Europe has relatively strong privacy and Data Protection legislation, there has been a surprising lack of willingness to enforce these laws. Prosecutions under the UK Data Protection Act are rare enough to be almost unheard of. As so often in enforcement, despite its weaker laws, the US has taken the lead:

- US service provider Verizon has been told in court that it should have foreseen the effect of the Slammer virus on its networks.
- A judge recently ordered the US Department of the Interior to close down its Internet links because it could not protect critical data.
- The pharmaceutical giant Eli Lilly had to promise to the FTC that it had improved its security after a breach revealed the email addresses of some 700 subscribers to their Prozac website.

The result is that in the USA, there is beginning to be at least a movement towards recognising a need to take positive action towards addressing information risks. The UK and EU, despite their stronger legislative frameworks, seem to be unwilling to take the step of actually pushing companies into compliance.

The Sarbanes-Oxley act on corporate governance definitely includes information risk in the scope of risks that must be clearly identified, reported and managed, and its European equivalent will surely do the same.

Whether this will finally be enough to overcome the reluctance of companies to treat information risk as a human problem rather than a technical one, and whether it will be a genuine spur to change or merely another good idea that gets ignored in the real world, remain to be seen.

<http://www.vnunet.com/News/1153867>

<http://www.informationweek.com/story/IWK20030130S0015>

http://govtsecurity.securitysolutions.com/ar/security_think_tank_gives/

<http://www.computerworld.com/governmenttopics/government/legalissues/story/0,10801,81879,00.html>

http://www.gcn.com/vol1_no1/daily-updates/24912-1.html

<http://www.theinquirer.net/?article=15014>

<http://www.vnunet.com/News/1153534>

<http://www.theregister.co.uk/content/55/36706.html>



David Biggins

David is the head of Information Risk at idRisk, a network of specialised, independent risk advisors.

View David's Profile: http://www.idrisk.com/risk_consulting_az.asp?id=15

About idRisk

idRisk is a network of specialised, independent risk advisors who are regarded as experts in their respective fields and who provide comprehensive, high quality unbiased advice on, and solutions to, all aspects of risk a company may encounter.

idRisk's Consultants come from an array of different backgrounds with diverse skill sets and experiences covering the broad spectrum of risk and its management.

By creating an extended network of highly skilled consultants and combining them with leading edge technology and information processes, idRisk can design, develop and deliver the best solutions to all major business risk areas.