An IT manager's insight into securing removable media

Removable media devices are here to stay. Their ease of use and low cost have made them ubiquitous in the work environment – but at what price? In this article **Magnus Ahlberg** looks at the pros and cons of removable media, and the steps businesses can take to mitigate the security risks.

When I last looked on the Internet to buy a USB memory stick, I found that for a few hundred pounds I could purchase a four gigabyte device the size of a pen. That's a lot of information you can now carry in the palm of your hand.

Thanks to their large capacities, portability and simplicity, removable media have become one of the most popular types of storage devices around today. You've only to go down to one of the big computer shows to be offered a free memory stick as a stand give-away. If you take part in a training course, you might be given one with all your course notes stored on it.

If you're like me, the advantages of using a small memory stick, Compact Flash (CF) card, or digital camera memory card are indeed enticing. Gone are the days when you have to lug your laptop around with you on every long journey or on spells away from the office. Just attach a USB stick to your key ring and you can carry all the documents you could ever need without that heavy, cumbersome laptop forever being in your shadow.

Removable media devices are a fantastic new addition to the constantly growing assortment of computer gadgetry that add convenience to the way we work. But at what price? As removable media grows in popularity, more people are using them in the workplace to store corporate information. Documents, databases, graphics, music, even films and video can be tucked away on these highly portable devices. Yet the security implications and risks of removable media are considerable and need to be seriously assessed.

What happens, for example, if you lose your key ring which happens to have attached to it a USB token containing all your downloaded – and unprotected – corporate documents?

You're in luck, of course, if it only gets picked up by an inquisitive passer-by who, after reading it, finds your information is of little interest. But what happens if the information is accessed by a criminal, journalist or competitor? The entire contents of your PC could find its way into the public eye. Worse still, you can get held to ransom by the opportunist looking to bribe you so as not to expose the information that he/she has found on your company.

> If you have no idea who is using removable media in your organisation, you have no idea who is downloading and removing your intellectual property and other sensitive company information.

Perhaps most devastating of all, you could find the entire contents of your bank account emptied or even have your identity stolen. These scenarios are very real and have the potential to be incredibly damaging.

If you have no idea who is using removable media in your organisation, you have no idea who is downloading and removing your intellectual property and other sensitive company information. You don't know where it is being taken, or what risks to which it is being exposed.

The harm to your business posed by information loss is not simply financial or operational. You must also consider the legal liabilities of information carried away on removable media. If a disgruntled employee decides to leak out information on your customers, you could find you are in for a very big libel suit, prosecution by data protection regulators, as well as significant damage to your company's reputation.

Although tremendously useful, removable media devices, due to their small size, guises and uses, can be a serious security threat to any organisation. Here are a few hints and tips on balancing the benefits of these devices against the risks they pose:

Step 1 – Security Policy

Removable media devices are not toys. Decide how you as a company want to manage them. It would be naïve to think you could simply ban all removable media. However, you should introduce removable media into your Security Policy and make sure that everyone on

your staff reads and signs the policy. Also, explain to your staff what actions will be taken if the policy is ignored.

Step 2 - Education

Inform your employees about security and its implications. Explain why certain controls have to be put in place. Do not just impose those controls or users will ignore them.

Step 3 - Encryption

Consider employing a mobile data protection product. Mandatory media encryption solutions are available that can be centrally controlled by the IT department. The best products are fast and transparent to the user, so as to not interfere with their real-time work. Such protection automatically encrypts all information loaded onto a USB token or other removable media. Access is granted only to the user who holds the password.

Step 4 - Control

Implement device and executable control solutions that enable you to control exactly what devices can be connected to a system and what executable files can and cannot be run.

Step 5 - Audit and Measure

Ensure that you carry out regular audits to find out who is using removable media.

In today's complex digital world, nothing about security can be guaranteed. But by following these few simple steps, you can mitigate your risk and show that you have taken adequate steps to do everything you can to protect the information that is being carried around on removable media devices. Once you do, you will be able to sleep at night, safe in the knowledge that your company is not the next in line for public humiliation in the tabloids for allowing a leak of valuable information.

AUTHOR:

Magnus Ahlberg, UK Managing Director, Pointsec Mobile Technologies

CONTACT:

magnus.ahlberg@pointsec.com, +44 (0)1638 555082, www.pointsec.com

Phishing scams, continued from p.15

"Rather than using usernames and passwords which can be easily captured by phishing attacks, they should be thinking about more sophisticated techniques," he says. He suggests solutions such as two-factor authentication where customers are required to provide two forms of identification – for example, the traditional username/password combined with a physical device such as RSA's SecurID tokens or the Unified Authentication tokens developed by VeriSign. Another option, says Allan, is to develop some "kind of mutual authentication" where both the customer and the company provide information to prove their identities.

Scouring the Internet

Phishing detection solutions could help businesses to respond more quickly to attacks. Aungate, a division of the Autonomy Corporation, recently launched a solution that works by analysing the text, images and hyperlinks within e-mails. After collating the information, it then assesses whether a particular company has been spoofed. "We scan huge amounts of e-mail," says Ian Black, Aungate's Managing Director, "and we're able to form an understanding of whether an e-mail is potentially trying to appear to be something that it's not." According to tests, says Black, a company could identify a specific phishing attack that spoofs its brand within 15 minutes of the e-mail being sent. It enables companies to quickly locate fraudulent websites and attempt to close them down.

But while there is increasing cooperation with law enforcement agencies in shutting down fraudulent sites, the process is not always as quick as it could be. Black says that some organisations have been forced to resort to denial of service attacks on spoof sites while they wait for the authorities to act. However, "law enforcement agencies are getting more adept at moving quickly," he says. US agencies have tended to lead in this area, and while there has been less agility in the UK, and even less in Europe, Black says they are "waking up fast to the problem."

Fast response times could drastically reduce the impact of a phishing attack. "But it isn't just a case of shutting the website down," says Black. "You've then got to communicate with your customers." And timing is crucial. The quicker the response, the greater the chance of minimising damage, but also reassuring customers that you are on top of the situation. "If you handle the attack poorly," warns Black, "you get attacked by your customers as well."

In it for the long haul

There is no doubt that phishing has become a pervasive problem, but while initially slow to react, industry has recognised the need to combat it across a number of fronts. Consumer education, technology, and cooperation with law enforcement will help to thwart some attacks. But don't expect it to solve the problem. Trends suggest that phishing is likely to follow in the footsteps of spam, which despite a concerted effort to stamp it out, still continues to plague the Internet. "Spam was the beginning, and the increasing sophistication of spam was the next step. And we're seeing that now with phishing," warns Black. "I think we are starting to see the ramp up of a huge increase in this sort of activity."

It is not perhaps the beginning of the end, but rather the end of the beginning.

AUTHOR:

Alan Pedersen, Editor, *Privacy Laws & Business International*

CONTACT:

alan@priavcylaws.com

USEFUL URLS:

Anti-Phishing Working Group
www.antiphishing.org

Autonomy/Aungate
www.autonomy.com

CipherTrust
www.ciphertrust.com

MailFrontier
www.mailfrontier.com

Ponemon Institute
www.ponemon.org

Truste
www.truste.org

RSA Security
www.rsasecurity.com

VeriSign
www.verisign.com