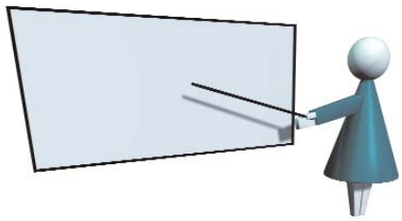


Intranets

Creating a secure intranet environment Part II

In the final part of this series on intranet security, Paul Chin examines the importance of security awareness and the employee's role in protecting their organisation's vital intellectual property.

By Paul Chin

WHAT GOOD is a state-of-the-art home security system if the homeowner forgets to turn it on, leaves the front door wide open or accidentally burns the house to cinders with a carelessly discarded cigarette? Security can't be solved by technology alone. Simple human negligence can be a detriment to any solution that is put into place.

While the theft of personal property will lead to monetary loss and emotional distress, companies have far more to worry about. A single careless action by an employee with valid network permissions can result in the divulging of trade secrets or corporate strategies.

It's important for organisations to realise that security can be compromised internally as much as externally – and it's not always through malicious intent. Corporate information can just as easily be leaked by human error or inappropriate behaviour. Employees need to play a part in protecting their organisation's intellectual property; technology should not be treated as a foolproof, security safety net.

So with all the technological mechanisms put into place to keep outside threats from adversely affecting infrastructure and information, how do we keep employees from burning the building from the inside out? It begins with awareness, education and a comprehensive security policy.

The value of intellectual property

Information can not be protected by technology alone. Regardless of the technological mechanisms implemented – data encryption, firewalls, access-control lists and user authentication – the weakest link is still the people on the other end of this technology. They are the ones holding the keys, literally and figuratively, to an organisation's intellectual property. And there is nothing that technology can do to prevent careless users from blurting out their network passwords.

Intellectual property is probably an organisation's most valuable asset. It is a mission-critical component often overshadowed by physical assets. But the value of these intangible assets shouldn't be measured with any less significance. Unfortunately, many organisations do not assign a monetary value to their information until litigation.

According to the report, *Trends in Proprietary Information Loss* – a survey sponsored by PricewaterhouseCoopers, the US Chamber of Commerce and the ASIS Foundation – 70 per cent of a typical US company's market value comes from its intellectual property. Although approximately three quarters of respondents stated that intellectual property and proprietary information are vital to their company's success, only 55 per cent were concerned about information loss and are taking active measures to safeguard their information. Among the areas at greatest risk are:

- Research and development;
- Customer information;
- Financial data;
- Strategic plans.

The loss of an organisation's intellectual property extends well beyond the immediate loss of money. It can have far-reaching consequences such as:

- The tarnishing of corporate image and brand;
- Loss of reputation;
- Loss of business;
- Loss of clients or potential clients.

It will threaten the company's livelihood, and possibly its very existence. Employees have an obligation to maintain the integrity of their organisation's intellectual property. But, despite this information's inherent value and importance, staff are rarely taught the correct way to handle information that's entrusted to them. When employees become more aware of the sensitive and valuable nature of their organisation's content, they will be less likely to treat it in such a nonchalant manner.

Tips on handling and protecting intellectual property

Security breaches and information leaks can be caused by 'dumb luck' as much as by design. It's not only hackers and disgruntled employees that do all the damage. A careless, albeit well-meaning user who is unfamiliar with proper content-handling protocol can unintentionally leak vital corporate information and not even know it until it's too late.

In addition to the technological mechanisms put into place to protect intellectual property, there are many procedural and practical ways to minimise the risk of exposing sensitive information.

Implement a strong password policy
The majority of users choose simple passwords – for example, birthdays, telephone numbers, names of family members or pets – so that they can be easily remembered. But these types of passwords can be guessed by hackers far too easily. Strong passwords exclude any plain english word and should contain at least five characters, using a mix of letters (both upper and lower case) and numbers. Servers should also be configured to lock accounts after a certain number of unsuccessful log-ins, in order to avoid repeated attempts with the same account.

The "sinful-seven" online activities according to Sophos:

- Downloading music and movies;
- Opening e-mail attachments or clicking on links in unsolicited e-mails;
- Surfing pornographic or other dubious websites;
- Running 'joke' programs sent by friends and colleagues;
- Installing unauthorised software and web-browser plug-ins;
- Giving information to unknown parties via phone or e-mail;
- Using the same password on different websites.

Source: www.sophos.com

Never transmit sensitive data over an insecure line
E-mail and faxes have made the transmission of documents easier than ever before. But users rarely give thought to how insecure this really is. Sensitive information should never be sent over an open fax line because there's no telling who is on the receiving end or how long it will sit on their fax machine. Documents sent by e-mail should always be encrypted to ensure that they are not intercepted and modified by a third party before reaching their destination.

Never leave hard copies in plain view
IT goes to great lengths to secure digital information from unauthorised access, but nothing keeps users from printing out this content and leaving it lying on the printer or on their desk. Users must always be conscious of the sensitive nature of their company's intellectual property – whether in bytes or in print. While the printing of confidential information can be controlled through digital-rights-management software, sometimes it is necessary to work in hard copy. All users with access to restricted content must be aware of the proper handling and disposal of these hard copies once they are printed.

Never leave 'keys' in the open
Anything that provides access to restricted information and resources – passwords, PIN numbers, combinations, ID cards or keys – should never be left out in the open. Employees who feel overwhelmed by the number of passwords they have to remember will often write them down on a piece of paper and stick it right next to their PC for the world to see. If staff have a difficult time managing their passwords and must write them down, they need to make sure they are locked under physical lock and key. Magnetic ID cards and keys used to gain access into secured areas or filing cabinets must be kept close by at all times. They should never be left on a desk where they can be picked up by someone else.

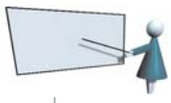
Take steps to secure information for transportation
When physical shipment of confidential information is necessary (for example, if the content is too large to send via encrypted e-mail, or when the content only exists in hard-copy format), steps must be taken to ensure secure transport of the medium – whether CD-ROM, USB flash drive or papers – with a reliable carrier or courier service. The recipient of the package must also abide by the sender's strict policy regarding the handling of sensitive material.

Grant access on a 'need to know' basis
Blanket access should never be given to sensitive information. The simple fact that two users belong to the same department should not be cause for equal access rights. Sensitive content must be granted individually on a need-to-know basis. This is something that should be decided and authorised by each individual intranet-section owner.

Implement a formal access requisition procedure
Access to restricted information must never be granted on an ad hoc or verbal basis. A formal procedure, whether online or paper-based, should be set up – whereby all access requests for restricted information must first be authorised by the content owner (usually an intranet-section manager). This has the added advantage of leaving an access-request audit trail.

Lock workstations with a password
Unattended workstations are a huge security hazard. Once users log on to the corporate network or intranet, passers by will be able to access anything available to the logged on user. This is akin to unlocking the door to your house and leaving it wide open. And if a passer-by should do anything illegal using one of these logged-in workstations, the original user will be held liable – since the actions are carried out using their credentials. To combat this, workstations should be

A careless, albeit well-meaning user who is unfamiliar with proper content-handling protocol can unintentionally leak vital corporate information and not even know it until it is too late.



configured to automatically lock after a period of inactivity.

Archive old information
Information that has reached the end of its lifecycle should to be disposed of securely by shredding hard copies and scrubbing hard disks. However, there are new regulations (such as the Sarbanes Oxley Act) that have redefined how long organisations must keep certain types of documents. If no longer needed, these documents should not be kept on an intranet, regardless of how secure the system may be. Instead, they should be archived off the system in a secured facility and environment.

Employees should be aware of social engineering
Social engineering is a non-technical method of gaining access to an organisation's network and information. It often involves the use of human interaction and psychology to get unsuspecting users to divulge personal and private information, which can then be used to gain unauthorised access to a company's network and resources. Social engineers often gather intelligence by gaining the confidence of their mark, appealing to their egos or exploiting their natural inclination to be helpful. Users should be made aware not only of the existence of social engineers, but also of their techniques, in order to be able to identify a con when they encounter one.

Employees should always be aware of their surroundings
Employees must be cautious of what they say and who they say it to in public places, where just about anyone could be within earshot. In the very real world of industrial espionage, corporate spies are known to gather intelligence by prowling taverns, restaurants and nightclubs that are frequented by employees of their competition. These spies are referred to as 'nightcrawlers' and are often attractive, highly personable and expert social engineers. They will use a mix of passive eavesdropping and active social engineering techniques to gather information.

The importance of a corporate security policy
Security of corporate information is as much an issue of management as it is technology. Every company needs to have a formal security policy outlining the proper handling of sensitive information – both inside and outside the company. While it would be nice to think that all employees will be conscientious in their handling of their organisation's information, we know that is not always the case. Even something that might seem benign, such as taking work home for the evening, can result in the exposure of private, corporate information.

A recent survey conducted by Sophos, a UK-based computer security firm specialising in anti-malware software, revealed that 79 per cent of IT professionals believe that employees are acting unsafely when online and, as a result, are putting their companies at risk. Sophos went on to describe what it refers to as the "sinful-seven" online activities (see sidebar on page 27) – activities that can have serious consequences, not only to an organisation's intellectual property, but its entire technological infrastructure.

Companies are responsible for educating their employees on the value of intellectual property and the risks associated with improper behaviour. Despite repeated warnings, both from their employers and the media, many employees still don't seem to understand the risks associated with opening unsolicited e-mail attachments or visiting questionable websites.

In another poll conducted by Sophos, 63 per cent of IT professionals believe that employees who fail to follow established security guidelines should receive an official warning, followed by dismissal; while 10 per cent of respondents feel that employees should be dismissed outright.

A corporate-security policy goes a long way towards minimising the possibility of an employee burning the company down from the inside out. It needs to be written in plain language with as little legalese as possible in order to encourage employees to read and become familiar with it. While every organisation's security policy will differ depending on variables such as company size, industry, and information types; the SANS Institute – a cooperative research and education organisation comprised of security practitioners in government agencies, corporations and universities around the world – offers an excellent example policy on its website: http://www.sans.org/resources/policies/Information_Sensitivity_Policy.pdf

It's important for organisations to realise that security can be compromised internally as much as externally and it's not always through malicious intent. Corporate information can just as easily be leaked by human error or inappropriate behaviour.

Covered on all sides
Information security requires a multi-pronged solution. A policy alone will not keep company information from leaking out, but neither will technology alone. But, by combining the two with some sound common sense, an organisation can greatly reduce the possibilities and the risks.

Employees need to learn to be diligent about not only keeping the doors locked, but also to conduct themselves, and their handling of information, in an appropriate manner. Sometimes an ounce of knowledge can be worth more than all the technology in the world.

Paul Chin is an IT consultant and freelance writer. Previously, Paul worked as an intranet specialist in the aerospace and competitive intelligence industries. He can be contacted by e-mail at: post@paulchinonline.com.