

Intranets

Creating a secure intranet environment **Part I**

In the first of this two-part series, Paul Chin promotes 'prevention' over 'reaction' and highlights some of the mechanisms that can contribute towards a more secure environment.

"IT WILL never happen to us." These are the famous last words that often precede the hair-pulling, teeth-gnashing stress associated with the loss of critical data, due to either carelessness or malicious attack. It's a false affirmation that marks victims like a war wound – a daily reminder of the reality of threats to information and infrastructure.

Security is one of those issues that every non-IT executive and intranet owner is aware of, but more often than not, hopes someone else will address. They naturally assume it's been dealt with by the techies down in IT, but this is the wrong attitude. It is their content that needs to be protected and they must be involved in the process.

Being relatively safe from outside threats, such as unauthorised access by malicious third-parties, doesn't necessarily mean all internal network resources are safe. Intranet security needs to go well beyond the corporate firewall. A truly secure intranet environment is a marriage of technology, policy and basic common sense.

Be proactive, not reactive

Most people, by human nature, are reactive. They are prompted into action as a result of some unfortunate incident. Take, for example, the amount of homeowners who purchase alarm

By Paul Chin

systems and insurance policies only after their houses are broken into and their property stolen. Although this might protect them from future break-ins, it is little consolation for what has already been lost.

When you're operating a corporate intranet this type of attitude is unforgivable. Consequences of a security breach, whether accidental or malicious, can include data loss and the divulging of trade secrets or other intellectual property to competitors or third parties that may wish to do your organisation harm. And, if your information and infrastructure are compromised your only recourse may be to take legal action. But this is a reactive measure – the damage has already been done and you will be left to deal with time-consuming and costly litigation.

According to the 2005 CSI/FBI Computer Crime and Security Survey (see box on opposite page), losses caused by unauthorised access and theft of proprietary information exceeded \$31m and \$30m, respectively. Only 27 per cent of respondents indicated that their organisation allocated more than five per cent of its total IT budget on security.

Rather than fall prey to this cycle of action and reaction, intranet owners must

place more emphasis on prevention. Many don't because they think it requires too much time and effort to prepare for an eventuality, but it's not worth the gamble. Just because it hasn't happened yet, doesn't mean it never will. The longer vital information and infrastructures are left unprotected – or, in most cases, loosely protected – the more likely they are to be compromised in the future.

Protecting your information

With all the high-profile media coverage of corporate-data loss and threats to system integrity, it is amazing that there are still those who believe in 'security through obscurity'.

The mentality behind this paper-thin theory is that if no one knows about it, no one will find it. Sensitive intranet content is 'protected' behind an unlinked URL, but this is the technological equivalent of hiding your house keys underneath the welcome mat and hoping that no one will find them. Unfortunately, while it may prevent casual users from stumbling across hidden content, it does nothing to keep away those who are actively seeking it out.

When it comes to critical corporate information – the heart of any organisation – you can not bank on ignorance for protection. Security must be based on concrete measures that will not only prevent curious users from stumbling onto something they're not meant to see, but will also withstand active system hacking. And the more sensitive your

Every piece of content should have a sensitivity classification.

intranet's content, the more elaborate these security measures need to be. Don't try protecting a million dollars worth of content with a two dollar lock that can be broken with a toothpick and a witty insult.

The most common way to control access to IT systems is still with the use of a username and password. But a password is only as secure as the person holding it. Systems can be compromised by careless users who write theirs down or pass them on to their colleagues (the issue of intranet-security policy and education will be discussed in the next part of this series).

A far more effective way to secure corporate resources is by combining two security mechanisms: something you have and something you know. Combining these two mechanisms provides far greater security in the event that one is lost or divulged (see table below).

But, regardless of your implementation preferences, all security mechanisms are based on the same digital questions that are found on any system's backend:

Who are you?

Whether in the form of a username and password combination, or a biometric scan, user authentication identifies the person trying to gain access to the system. If the system recognises the person as a valid user, it will ask the next question as they navigate the site.

What do you have access to?

An access control list (ACL) tells the system which users have access to what content, and what they are allowed to do with it. Some users will have read-only permissions, while others will have access to edit the content as well.

Intranet security models

Intranets are often referred to as one-stop

The 2005 CSI/FBI Computer Crime and Security Survey

The 2005 CSI/FBI Computer Crime and Security Survey is an annual survey conducted by the Computer Security Institute (CSI) and the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad.

The results of the survey, which is now in its tenth year, are based on the responses of 700 computer-security practitioners in US corporations, government agencies, financial/medical institutions and universities.

A PDF of the entire report can be downloaded from CSI's website at: www.gocsi.com.

shops that provide an organisation's user community with all of its information needs, in a shared, centralised environment. They house data and applications catering to numerous departments and workgroups. With so much traffic flowing through, you need to ensure that only selected users can access this content.

Establish content sensitivity

Intranet content and application sensitivity plays a very large role in determining a proper security model. Every piece of content should have a sensitivity classification. Some information will be openly available through any public medium, while some will need to be secured from all but a small group of users.

But remember that, although you want your intranet to be protected from unauthorised access, you don't want to be so restrictive that the system becomes unusable. For this reason, make sure that intranet security is proportional to content sensitivity. The various levels of content-sensitivity classifications are:

Public content

Content that is openly available and can be found on any public medium (for example, websites, magazines and newspapers). Public content can be published

on an organisation's website as well as its intranet site. Since this content is publicly available, there is no need to secure it.

Examples: Press releases, product and/or service information, job listings, financial reports for publicly-traded companies.

Company content

Company content is available to all employees of an organisation, but not to the public. This type of information must be secured from any external access, but is open to all members of the organisation's internal network.

Examples: Employee reference manuals, corporate policies, internal forms.

Restricted content

Restricted content is only available to certain users and groups that are directly involved in the activities that the content relates to. Access could be based on department, projects and contracts or specific work groups.

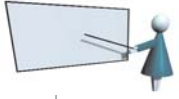
Examples: Corporate strategies, client lists and contact information, research and development. Project and contract specs.

Determine intranet access

Security is not black and white, it is granular. As such, access to intranet content must be granted on a user by user, need to know basis. It must never be allocated in an 'all or nothing' fashion.

The best solution is to implement a multi-tiered security model. I often liken intranet security to that at a hotel. You want all clientele to be able to get into the hotel through the front door, but not into every individual room – and most certainly not into guests' luggage.

| Examples of things you have: | Examples of things you know: |
|--|---|
| A physical key. A badge used for magnetic readers. Your fingerprints, retina, iris, voice and facial pattern (used in biometric scanners). | Your username. Your password. A numeric pin number. A pass-phrase. |



Intranet access types

General site access: 'The hotel's front door'

General access is the lowest-level intranet access granted to users. They will be allowed to enter the systems 'front door' and read (but not modify) all non-sensitive content.

Secured sections access: 'The guest rooms'

These are the individual intranet sections that are secured from basic, general-access users. Secured sections contain sensitive content that should only be accessible to those directly involved in the activities associated with the content. Access to secured sections is usually authorised by that section's content owner and put into effect by the systems administrator.

Content editing access: 'Housekeeping'

Content owners and editors – those responsible for populating and managing their section of the site – will have access to add and modify content for their respective sections.

System administration access: 'Hotel management'

Administrative access is the highest level of intranet access and must be limited to only a few select individuals (usually members of the IT staff). Those with administrative privileges will have access to the entire system. This includes all secured and non-secured content as well the intranet's backbone, such as the physical server(s) and the development environment.

Grouping resources and access rights

Content with similar context and sensitivity should be grouped together whenever possible. This not only eases management of security, but also minimises the potential for human error.

Security should never be handled on a file by file basis, especially if the files are mixed in among other non-secured content. Instead, sensitive content should be grouped in a centralised-location and secured as a whole. The same principle should be applied when granting access rights to users. Instead of granting single users access to various intranet resources, they should be put into logical groups with similar access rights. Access to sensitive content is then given at the group level. This way, if a content editor in HR leaves the company, administrators can simply remove that user's account from the HR group, rather than having to locate all the resources that user had access to.

Security involves everyone

Securing corporate content is a collaborative effort. While IT is responsible for implementing the technical aspects of intranet security, it is down to the content owner to identify what needs to be secured and who should have access to it. After all, no one knows their content and users better than the content owners themselves.

Security, like the proverbial chain, is only as strong as its weakest link. Without the co-operation of IT and all intranet content owners, system integrity and, in some extreme cases, organisational stability can be threatened because of a single weak point. And, undoubtedly, everyone will feel the effects should the chain break. ■

Paul Chin is an IT consultant and freelance writer. Previously, Paul worked as an intranet specialist in the aerospace and competitive intelligence industries.



For more news, case studies, opinion and analysis, visit the ei magazine website at:

www.eimagazine.com