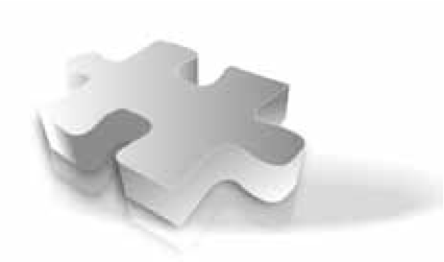
7

Essential steps to Securing Intellectual Property

A CommsNet Group Best-Practice Guide to ensuring business availability, performance and security

CommsNet Group

Co Written by
Dr David Garrard and Boaz Fischer



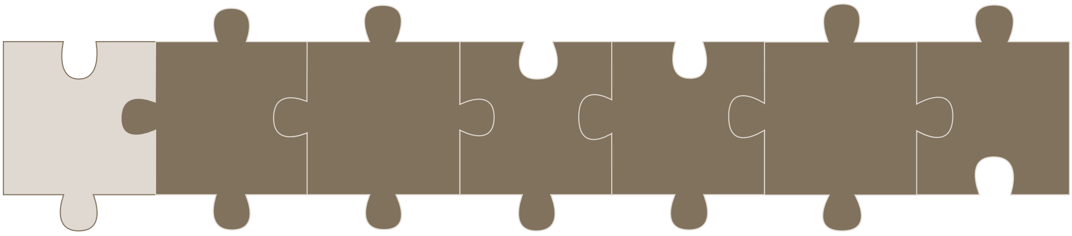
You do have the right to offer this report for free, offer it as a bonus, give it away to your clients, partners, suppliers, friends and business associates. You can also send this material as part of your sales and marketing strategies. You also have the right to pass these rights along to anyone who receives this report.

You do not have the right to change the content in any way or quote it without giving credit to the authors.

Enjoy

Boaz Fischer
Managing Director

CommsNet Group



Introduction

Intellectual property represents the property of your mind or intellect. It can be an invention, trade mark, original design or the practical application of a good idea. In business terms, this means your proprietary knowledge - a key component of success in business today

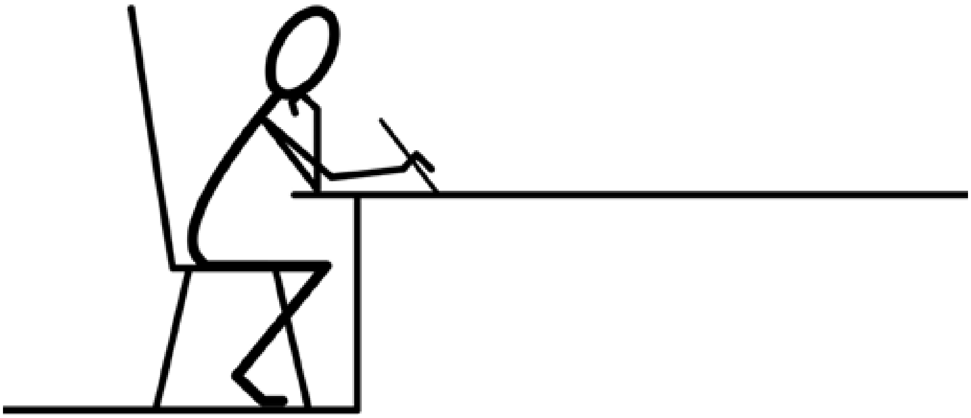
Why should you care about intellectual property? It is often the edge which sets successful organisations apart and as world markets become increasingly competitive, protecting your intellectual property becomes essential.

To give some examples, does your business produce a unique product? Does producing this product require special processes that are unique to your business? If the answer to this question is yes than you have intellectual property.

Here are a number of critical questions that you need to ask yourself:

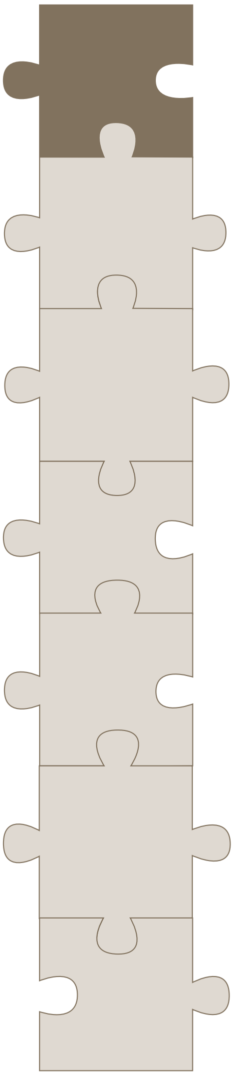
1. What would happen if your intellectual property were lost?
2. What would happen if your intellectual property were stolen?
3. What impact would it have on your business?
4. Could your business go into default?
5. What impact could it have on yourself and your family?

The purpose of this white paper is to suggest a security strategy methodology in order to protect your organisations intellectual property (IP) against most common threats.



Step 1

IP Classification



The first step in protecting your companies Intellectual property (IP) is to identify IP classification by using the 5 W's +H process questionnaire:

- **W**ho within your organisation is developing or accessing IP?
- **W**hat IP is it?
- **W**hen was it last used?
- **W**here it is stored?
- **W**hy is it stored there?
- **H**ow is it accessed?

Any product of creative efforts that directly contribute to the product your business produces is IP. Intellectual property can be classified in the following areas:

- Copyrights
- Trademarks
- Patents
- Industry designs
- Rights
- Trade secrets
- Processes
- Designs

The next step in protecting IP is to perform a threat vector analysis to identify the threats to the IP and implement controls to counter these threats. Once the IP is classified it is now time to consider each threat vector and determine appropriate countermeasures.

Step 2

Understanding Threat Vectors

Before we can discuss threats to IP and the appropriate counter measures, we need to discuss the classification system for threats and their method of delivery threat vectors.

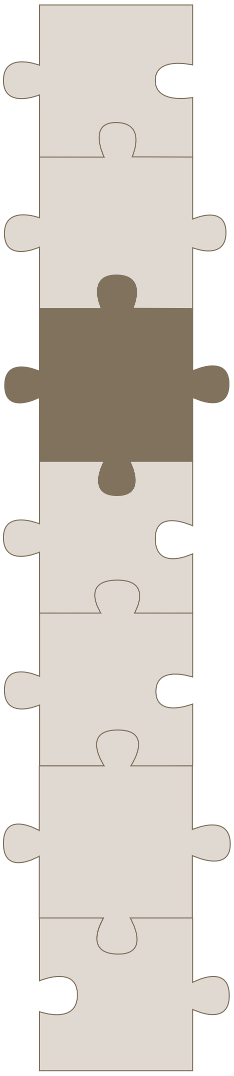
A threat is the occurrence or probability of occurrence of adverse event that puts the possession of your organisations IP at risk. A threat vector is a mechanism via which that threat can be delivered. The common threat vectors are the following:

1. Access by telephone;
2. Access by external networks;
3. Access by internal networks
4. Physical access;

Let us now discuss high level counter measures for each threat vector.

Step 3

Protecting IP from Telephony Threats



Can the IP be accessed via the telephone? Remember in the age of the Internet this could be systems like Skype.

What you need to consider:

- Is there a business requirement for allowing Internet based telephony into you network? If the answer is no, then block Internet telephony at your firewall.
- If there is a need for your IP to be accessible via modems then you need to put in place controls on who can access this IP. Some examples of these control mechanisms are as follows:
    - Use a dial back modem, these devices disconnects after the user authenticates and dials back a stored number;
    - Implement some form of password protection with the password changed on a regular basis;
    - Consider encrypting the IP so as to provide an extra level of security.

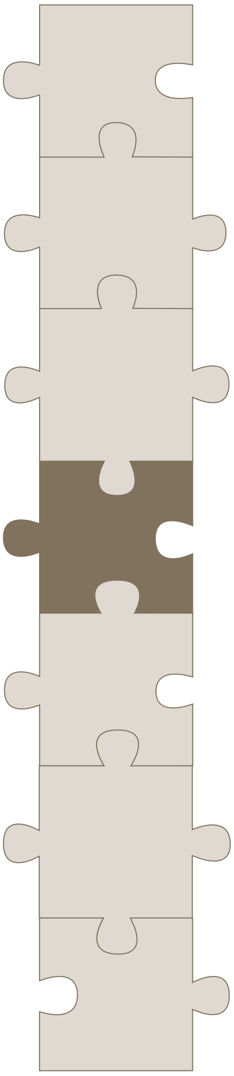
Step 4

Protecting IP from Access via External Networks

Today, the primary external network used to access corporate data is the Internet. If any of your company's intellectual property is on a computer system accessible by the Internet, here are a few steps that you need to consider:

- Is there a valid business reason for it to be there? If not, move it to a system that is backed up but is not available from the Internet.

- If there is a valid reason for the IP to be available on Internet, then the following controls will be helpful in protecting the IP:
  - Consider implementing the controls discussed in the previous session such as passwords and encryption
  - Consider using the security capabilities of the computers operating system to restrict access to the IP
  - Another control is to consider the use of data leakage protection systems. These systems allow you to mark you IP and prevent it or parts of it being sent out by email or file transfer and provide an audit trail of who has access to the IP
  - With the increasing use of iPhones, iPads and other related smart mobile devices consider implementing an enterprise system that can set limits and enforce polices on what can and cannot be stored and accessed by these devices
  - You should back your data up on a regular basis especially your companies IP. Where and how securely are those backups stored? If you backups can be accessed so can your company's IP



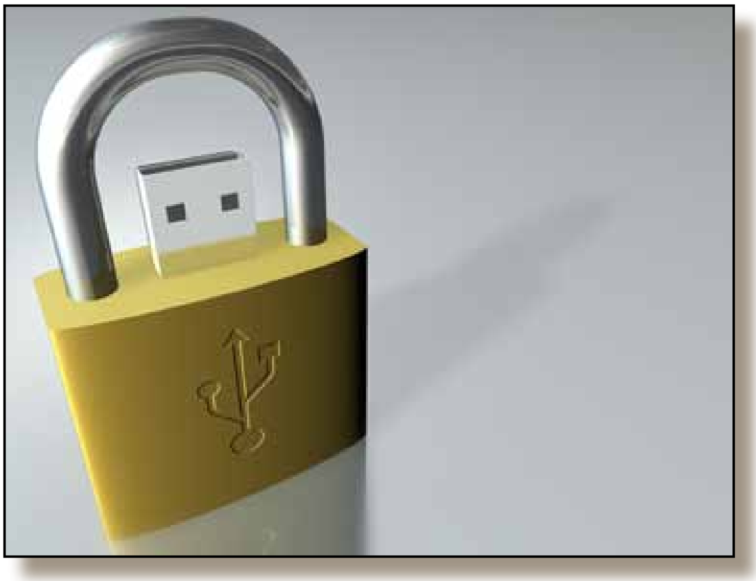
Step 5

Protecting IP from Access via Internal Networks

Another possible thereat vector for your IP is access by persons on your internal network.

People can store the IP on a USB stick and walk out the door or send it out via social media networks. Fortunately there are controls that can be implemented to protect against these threats:

- Consider implementing the controls discussed in the previous two sections
- Ensure that you have polices in place specifying what your employees can and cannot do with your organisations intellectual property
- Consider the use of endpoint security software that can monitor what is transferred to and from USB devices or completely disable USB devices
- Ensure that every computer system has up to date antivirus software installed and it is kept up to date
- Consider using a web security gateway that can monitor exactly what applications and users are doing over the Internet
- Ensure that all devices on your computer systems are patched to the appropriate levels
- Consider implementing two factor based authentications systems rather than just password systems. One of the biggest weaknesses in password protection schemes is human nature. If people have too many passwords to remember, they will tend to use the same password or they will use easy to remember and guessable passwords. The weakness in human nature will be the most likely reason that an organisation will lose IP rather than deliberate abuse or error on the part of your organisation



Step 6

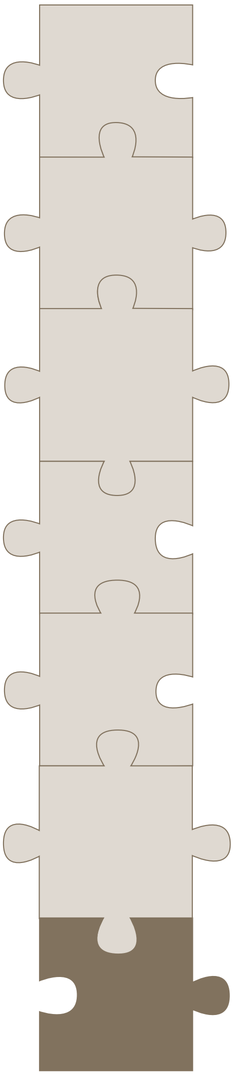
Protection IP from Physical Access

This is the hardest threat to counter because once someone has access to a physical asset they can usually bypass security controls in place. The following controls will assist in minimising physical access problems:

- Does the intellectual property need to be in an area that has unrestricted physical access. If there is not a valid business reason then consider moving the IP to a physically secure environment
- Consider implementing the controls outlined in the previous sections
- Review the physical security of where IP is stored and consider putting in place appropriate locks and a policy to control and log who has access to the keys of those locks
- Consider running a six monthly security audit and assessment on your current physical environment

Step 7

Protecting IP via Education and Policies



The final step in protecting your IP is not technical at all. These counter measures address the most complex challenge when you try and protect your companies Intellectual Property.

The challenge facing your organisation, alluded to in a previous section of this document is your users. If your people do not understand what your organisations IP is and its importance they will not take the appropriate due care to ensure adequate protection of your IP.

CommsNet Group recommends having twice yearly workshops with your people to discuss IP, raise security awareness and discuss the counter measures in place to protect IP and its effectiveness. By actively involving your people you will ensure that they take the extra steps to safeguard your IP.

Further steps you need to take to ensure that your IP is protected and to make sure that you have the appropriate security policies in place:

- Who has the responsibility to ensure that your organisation IP has the appropriate security policies and processes in place?
- What can and cannot be done with the organisation's IP?
- What is the expected duty of care your people must undertake when handling your organisation's IP?
- How are these measures and practices delivered to end users so that they can be effective in ensuring organisation IP is protected?

These polices need to be linked to your HR policies. A successful policy on handling IP must have direct and enforceable consequences.

Summary

The above seven steps summarizes simple processes to implement simple techniques for protecting your organisation's intellectual property.

As you can see, protecting intellectual property is not only vital but quite a complex business. CommsNet Group has many years of experience in assisting clients with protecting businesses intellectual property. Please do not hesitate to contact us if you would like to discuss what has been covered in this article or are seeking help in IP protection.

Final Remarks

At CommsNet Group, we have been involved in helping organisations in delivering technology and security peace of mind.

Our relationship with best in class technology and security vendors provides us with the ability to effectively focus in solving challenges and fostering joint success outcomes.

Our high quality process systems provide us with the ability to consistently deliver results effectively. Thus engendering greater productivity and more free time to focus on what is important.

Our people are highly customer focused, knowledgeable, experienced and delivering guaranteed and trusted supported services.

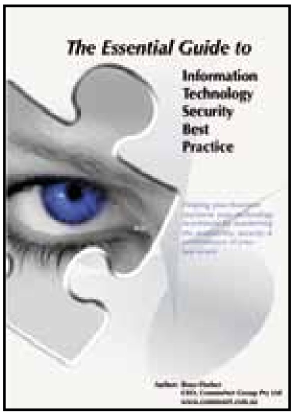
Our training enhances user awareness and increases their knowledge so that users can best use the technology that has been invested in safety.

Talk to us about simplifying your organization social networking practices. Or simply visit our web site **www.commsnet.com.au** to see how we deliver **Security Peace of Mind**.

About CommsNet Group

CommsNet Group Pty Ltd is an Australian owned company providing **Technology Peace of Mind and Security Peace of Mind** to organisations that depend on technology for their business needs, and operations who want to make certain that their systems are maximised for performance, systems are user friendly and easy to use, who wish their systems are 99.99% available and robust, users are empowered and productive and a fully 100% peace of mind money back guarantee.

For a further highly informative and practical step by step guide in gaining Security Peace of Mind, download **The Essential Guide to Information Technology Security Best Practice**.



In this guide you will find the following:

- The 7 key facts about security
- The 5 minute questionnaire that will reveal all your business security weaknesses and what you can do about them.
- Simple step by step processes to help you solve identified security concerns
- How to manage risk for each security concern
- A quick self security assessment that you can do in 5 minutes that will reveal your organisation's security health status
- How to embed a security culture within your organisation
- How to build an investment case for security that will be signed off by your senior management.

Visit http://infostore.saiglobal.com/store
Search under the following number: CN 001-2010