

Internet Security and Acceptable Use

IT support, even before you need it



Myths about IT that could sink or float your business- And what you can do to flourish instead

Introduction

Business owners and managers face a daily problem of ensuring their links to the Internet do not become pipelines for Malware, SPAM, Viruses and other internet sourced security threats. They often feel “it won’t happen to me” when considering issues such as virus outbreaks and malware / spyware infections.

The dilemma is that the Internet is both a salvation and the most likely way a business will experience downtime in terms of failed PCs or lost data. The Internet will offer a new way to trade, communicate and grow; however, it is also the most likely way in which an unsuspecting user will receive mail with a virus attached or the route via which innocent Web browsing may lead to the downloading of malware to the local PC.

What needs to be considered are the possible solutions to this problem, and to dispel myths regarding protection. The key myth is “**I have Anti Virus software so I am OK**”. Well, not by a long distance. Viruses represent a shrinking percentage of the overall risk to business security and so you should not cover this aspect alone. For a true level of protection you will need to consider Malware threats, SPAM and





Abussi Ltd. provides small and medium businesses with the high level of IT support larger companies enjoy, without the high level of investment. Instead of employing an expensive in-house IT department, Abussi partners gain unlimited support from an entire staff of qualified experts. Our services include consulting, implementation, support, monitoring and maintenance of your IT systems, all for an affordable monthly rate. Our solutions will save you money, decrease downtime and allow you to focus on what matters most – your business.



Help!

When you need it,
and before you
need it.

 Computer viruses *are not* the only threat to your business.

 Get a simple solution that protects you from everything out there.

Intrusion Protection (Firewall), plus a few others along the way. If you have antivirus software installed (and it's up to date) then great, but you should also consider the other elements to ensure you have a well protected network and internet link to your building.


Malware is difficult to deal with as it is 'hidden' within standard Web-page's and other legitimate sites. Therefore you need a product that can examine the Information as it arrives over the internet connect rather than wait for it to install itself and only then remove it (as sometimes it can't).


SPAM is another problem. Many e-mail programs such as Outlook have Junk Mail folders but this downloads the mail and then places it in a local folder, rather than using a tool which puts email into a safe place until you can decide what to do with it (delete or accept). This option is called quarantine and helps to place the mail away from your PC until you decide if it is legitimate or not.

Finally the option of protecting against hackers is achieved by the well known (but often little understood) provision of a Firewall.

The best solution to these 'blended threats' is to provide a mass of solutions to cover all of the risks, or a single solution that is multi-layered and which offers protection in all areas. The latter is the preferred solution and is the way larger companies protect themselves against these risks. More recently it is becoming more and more cost effective for smaller businesses to install a similar solution. You need to look for suppliers who provide devices called UTM devices (Unified Threat Management) as they have protection and security included to cover the 4 key areas we outline here, plus many more.

One of the best current offerings is available via a company called Untangle, who provides a single gateway software solution which can be loaded onto a standard PC and then acts as a gateway or sentry over your Internet connection.

 Small threats can become big problems.

 Control the content that goes in and out of your business.


The Untangle solution offers added protection as it is built upon Linux software, which in itself is less susceptible to hackers and viruses.


However, a recent release of the Untangle software can be downloaded to Windows and run on your normal PC alongside any other Anti Virus software you have installed.

So, if you run a small business, you should consider what to do in order to deal with these daily threats that may go unnoticed in your business, but which may create a long term problem. And that's the basis of this White Paper, to set out why implementing a general structure for Web content control within a business setting is so important. It's not all about the technology, like so many other business IT issues, it's about managing the IT in the context of other services such as HR and staff policy.

And with this in mind that's why this White Paper takes a long time to outline why Content control in the most general of forms (not just Technology) is so important to understand. Get it right and you have a good, well-rounded set of policies and instructions for your staff to follow on a day-to-day basis. Get it wrong and you have a potential legal nightmare in which neither you, your clients nor your staff has a clear understanding of what is allowed or how their actions may affect the overall security of your business.

Before digging into the detail, it is important to understand why so many companies today have chosen to consider enhanced Internet control solutions.

 Many Web sites can be very dangerous to the security of your business.

 Don't let social networking sites decrease your bottom line.

Why Implement Content Control ?

There are four main problems that content control can help solve:

Malware infections of your network – The Web has surpassed email as the main route for desktop and server infection. Google scrutinized 4.5 million Web pages and found that one in 10 contained malicious code that could infect a user's PC. Many of these pages are related to porn and free offer sites, but can also come through infected Web servers and the download of executable files. Content control is one of several layers (e.g. anti-spyware, anti-virus) that are needed to secure today's small business networks.

Google searches Web's dark side

<http://news.bbc.co.uk/1/hi/technology/6645895.stm>

Friday, 11 May 2007


Malicious code rise driven by Web


<http://news.bbc.co.uk/1/hi/technology/6591183.stm>

Wednesday, 25 April 2007

Misuse of employee time – excessive time spent on personal Web surfing, especially on addictive sites such as MySpace, Facebook and YouTube, can take a toll on an employee's performance. Salary.com reported in 2006 that the average worker admits to spending nearly an hour a day outside of lunch and breaks surfing the Internet for personal reasons – a truly astonishing figure!

Misuse of company resources – excessive bandwidth use, and the use of corporate server space to store large amounts of personal downloads, can be expensive and slow down the entire network, especially for hosted applications. Peer-to-peer software used for gaming and music sharing is notorious for crippling networks because they consume a disproportionate amount of network resources by opening multiple connections.

 Even the best employees abuse office Internet use.

 Take the “Big Family” approach to managing your employee Internet use.

Liability – inappropriate content on the network, especially pornography, can lead to a hostile work environment and ultimately a lawsuit.

These four types of problems incorporate a wide range of cultural, social, legal and commercial concerns. Thus, policing your network is not simply a case of thinking of all the possible forms of abuse that might exist and dealing with them individually. Rather, it is a case of integrating a clearly defined policy with sound network administration and sensitive management of staff.

The five-step planning structure we present, therefore, is aimed at balancing the needs of your network, your organization’s legal requirements and the recognition that the Internet is part of your employees’ everyday lives. It is important to keep in mind that staff may resent an overly restrictive policy. Nevertheless, each company needs to decide for itself where to draw the line between acceptable and unacceptable network use.


Write the Policy

Before sitting down to write the policy, you must first decide your goals for implementing Web control and an acceptable use policy. At a minimum, it should be to keep malware and inappropriate content off your network. This generally includes pornographic sites which are both inappropriate and a common source for malware. The measure here is that, if blocked, no reasonable employee is going to raise his hand in a company meeting to ask why he can’t access Playboy.com anymore. We term this type of company with minimal restrictions as “Big Family.” The philosophy can be summed-up as follows:

We consider our employees to be part of one big family. We trust them to manage their own time and commitments. We provide them a lot of latitude in how they meet their objectives.

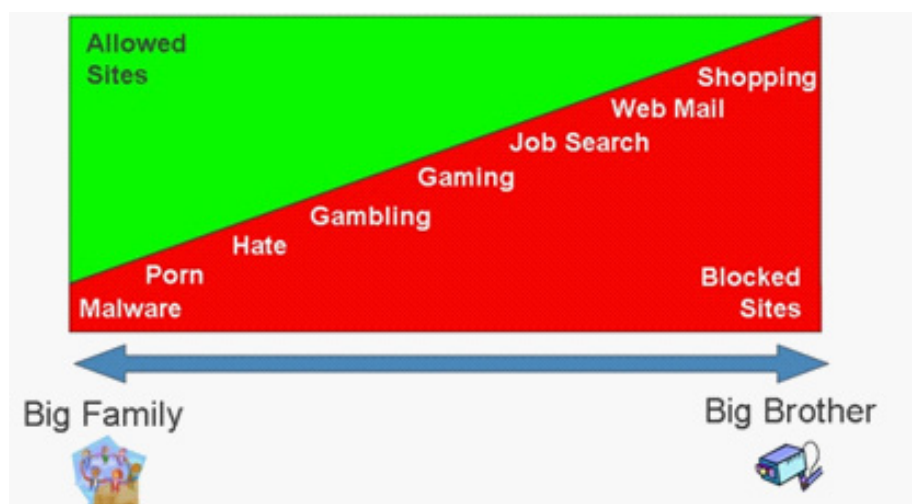
On the other extreme of the continuum is what we term “Big Brother.” This company blocks all Websites except for those work-related sites explicitly approved and added to the pass list. The philosophy is:


Internet Security and Acceptable Use

 The “Big Brother” approach to Internet security is much stricter.

Our employees are being paid to do a job, and we expect them to be productive at work. We do not want to see them staying late because they did not accomplish their tasks during the day, and we definitely do not want to be paying overtime because they were surfing the Internet for personal reasons.

Between Big Family and Big Brother, there is an entire range of companies who draw the line between acceptable and unacceptable network use. See Graph.




 When you decide which Internet policy is right for your business, write it down!


Some companies maintain multiple policies; one to provide free access based on time of day, such as during lunch, or by category of worker and one at other times.

Once you have decided what is and isn't acceptable use, the creation of a written policy is rather straightforward. There are, however, a few best practices to keep in mind.

Use clear and non-technical language

This can sometimes be a problem if the person(s) drafting the document are from a technical background and might have a different perspective on what is network abuse and what is not. Non-technical users are often unaware of how their activities impact bandwidth, how attachments sent via Web-mail might bypass corporate virus scanning, and how downloading a free screen saver can infect their computer with malware.

 Make sure your employees understand the Internet policy.

 Most Internet policy rules are common sense. Be sure to outline those that aren't!

Keep it short

The shorter the policy, the greater the chance that it will be read, understood, and referred to in the future. The goal is to have a policy that employees find easy to use and understand.

Stress the spirit of the law rather than the letter

Base your policy on simple principles that can be seen as reasonable by both technical and non-technical staff members. As a minimum, those principles should include the following:

- Although a certain amount of personal Internet use is acceptable, it should be kept to a necessary minimum and not impinge on the user's ability to do his / her job;
- Accessing pornographic, violent, abusive or hate sites is unacceptable;
- Using the network to harass or bully other staff members is unacceptable;
- Sending or posting confidential material, trade secrets, or proprietary information outside of the organization is prohibited;
- Sites, defined by the network administrator, deemed to be a security risk or excessively demanding of network bandwidth should be avoided;
- Staff should not expose the company to litigation for copyright infringement, by engaging in activities such as pirating music, videos, or software.

A company-specific policy can be based on this list and adapted as necessary for the circumstances. Keep in mind that the Internet is changing rapidly, and it would be tedious to rewrite the policy every time a new technology or phenomenon like MySpace presents itself as a threat. By clearly articulating a small set of guiding principals, you will avoid having to constantly revisit and rewrite the policy in the future.



Don't assume your staff is as tech-savvy as you are.



Monitoring increases the likelihood of employee Internet compliance.

Educate the Team

There is a need for training during this process. Staff who are aware of the exact nature of the threats that the Internet poses – and the issues of security and proper behaviour that accompany access to a company network – are more likely to accept and comply with the new policy. Additionally, they will be better equipped to obey the spirit of the policy, make intelligent decisions when surfing the Internet, and avoid malware traps.

Policy implementation training should ideally cover five areas:

External Threats

If your policy contains restrictions on employees' online actions in order to protect your network from spyware or virus outbreaks – and it should – you should spend some time explaining what form these threats might take and why specific provisions exist in the policy to prevent behaviour that might leave the network vulnerable.


Monitoring


Staff who are aware that network monitoring is taking place (or even possible) are much more likely to comply with the policy, including those parts that govern acceptable online behaviour. It should be made clear that everything staff do on the corporate network and every Web site they visit is visible by the administrator and traceable directly to them.

Although it is probably undesirable to overplay the “Big Brother” hand, you will usually find that a simple awareness that their online actions are subject to monitoring will prevent the vast majority of incidents of staff accessing inappropriate material.

Bandwidth Issues

An explanation that bandwidth is limited, that a slowdown affects everyone on the network, and that it costs money to add additional broadband speed should help to underline prohibitions contained in the policy. It should further be explained that peer-to-peer applications used for music sharing and gaming are notorious for clogging networks because they

 Let employees know that Internet misuse can lead to legal reprimand.

 Downloading should be closely monitored for the safety of your business.

open multiple connections to grab more bandwidth.

Issues Under Law


This topic covers three main areas that can mostly be avoided with good common sense.

First, the viewing and sharing of inappropriate material can create a hostile work environment. 'Inappropriate material' includes all images, cartoons, and messages that are sexually explicit, contain ethnic slurs, or promote racial, religious, or gender stereotypes. Viewing and sharing this material can lead to litigation.

Second, if an employee uses corporate Web access to post malicious, defamatory or libellous material on the Internet, a court may decide that the company is jointly liable with the poster, on the basis that it provided the means for him or her to carry out the act. Employees should be strongly discouraged from any action, private or business-related, that might invite litigation. On a related topic, it may well be useful to point out that email is a comparatively insecure mode of communication. Private opinions written into an email, even after being deleted, can easily be recovered in a forensic investigation.

Third, employees should never download or install unlicensed software of any kind. Doing so exposes the company to litigation and the network to risk. A recent pirated version of Windows Vista, in addition to being illegal, contained a virus that infected the host computer. Employees should be instructed to avoid downloading pirated and DRM (digitally rights-managed) material on to the corporate network.

Media files from services such as Apple's iTunes are generally licensed to the downloader's personal computer, and not to a company network. The presence of this sort of material on a multi-user network, even if it is kept secure from most users, will almost certainly be a breach of the vendor's terms and conditions – and, once again, the company may be jointly liable with the user should the vendor seek redress in the courts.

 Learn and explain what a “safe” password is.

Password Security


Although not traditionally part of a policy, an overview of password security is always a useful part of any IT training program, especially if you use any hosted applications. Employees should be told why it is a bad idea to share passwords or to use easily guessable ones.

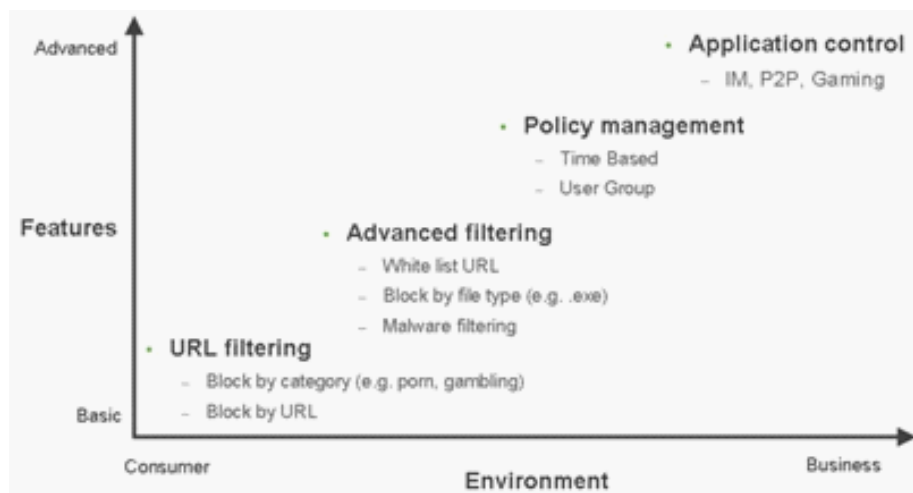
How the training is carried out depends on the nature of your company. However, it is important that technically-oriented trainers do not overestimate the technical sophistication of the staff. It is, therefore, advisable that at least some live training takes place, providing the opportunity for a question-and-answer session with staff. This is likely to be much more effective than simply distributing a booklet or email. However, given that some of the information is relatively complex for IT novices, having an online or printed resource file that everyone can access is also useful.


Implement Monitoring and Web Filtering


Once you have decided what is and isn't acceptable use, you need to identify a technology that will support your policy and business requirements. For example, will everyone fall under the same policy or do some employees require broader access to the Internet than others? Did you want to adjust the policies based on time of day? In addition to Web filtering, do you also want to restrict peer-to-peer applications such as Instant Messenger? Are any of your computers shared by multiple users requiring different policies based on log-in?

Further, Web filtering and the part of the policy that governs it must take into account the extent to which employees need to use the Web for work purposes. Essentially, it's important to decide whether restrictions should be placed using a system of blacklisting (i.e. employees can visit all sites except those specifically banned by name or by predefined category) or whitelisting (i.e. all sites are banned, except for a few that are useful for work) as might be the case in a retail or clerical environment.

 With Web Filtering, you decide which sites employees can visit - who, when, why and where.



 Make an example of employees who aren't following Internet usage policies.


 Keeping up with Internet trends allows you to monitor more effectively.


Filtering works best when combined with network monitoring. A brief but structured set of all users usage reports at set points during the working week should be sufficient to identify potential trends and problems as they arise. Beyond being good practice, it lets employees know the policy is being fairly applied.

When it comes to monitoring the Web access and behaviour of employees, probably the most efficient strategy is to take regular review reports and any individuals who give cause for concern can be subject to further monitoring, a warning, or disciplinary.

Perform a Periodic Review

It's vital to remember that technology in general and the Internet in particular are evolving rapidly. Given the increasingly social nature of the Web, such changes and opportunities are increasingly likely to register with younger team members before they come to the attention of senior management. As such, network managers need to stay on top of trends, monitor network activity, and be prepared to adjust the policy as necessary when new threats emerge. Many of these trends will first show-up in the reports. It is recommended that the policy is reviewed at least bi-annually to address emerging challenges. As the policy is updated, changes should be communicated to users.

 Have a clear, readable policy so employees know exactly where they stand.


 Policies should include harsher punishments for bigger Internet policy crimes.


Manage Incidents

Along with a clear policy, it's important to think through a plan for dealing with incidents and, better yet, to write it down. You should experience fewer problems if everyone is treated consistently and knows exactly where they stand.

We recommend a simple four-stage process to manage most infringements of the policy. The full process is designed for dealing with low-level, persistent offenders. It is anticipated that more serious infringements of the policy would immediately pass to level two, three or – in the case of the most serious abuse – four.

1. When a potential problem is noted with a particular employee's Internet use or network behaviour, the administrator takes steps to monitor that user's activity more intensively over a set period of, say, two weeks. The employee may not be informed, but it is probably useful to give him or her a short, informal, verbal notification that concerns have been raised and why certain behaviour is not acceptable. Whether or not such action is documented at this stage should depend on the nature of the infringement and your policy.
2. Persistent abuse, or a more significant infringement, should attract a formal, verbal warning from HR. This warning should be documented. Additionally, training and support should be offered to the employee to help him or her avoid future infringement.
3. Continued persistent abuse or serious infringement should attract a written warning from HR, with full documentation and appropriate retraining.
4. Habitual abuse and the most serious infringements – accessing serious or illegal pornography, for example – need to be dealt with by HR and higher levels of management. Cases at this level of seriousness can result in litigation should the employee resign or be dismissed. It is therefore vital that every step is documented and a number of different managers are involved in making judgments about the level of the seriousness / threat. If there is any suspicion that a crime has been committed, law enforcement should be notified.

 Employee awareness is the first step in implementing a fair Internet usage policy.

 Make sure you're covered with an Internet usage policy before it's too late.

The importance of employee awareness of the exact disciplinary structure, and the necessity of maintaining documentation, cannot be overstressed. Having clear procedures – especially governing how incidents are reported up the management chain – can also help to avoid problems in the event that a relatively senior individual is engaging in behaviour contrary to the policy.

Get Advice From An Expert


Look up a reputable IT provider for either one-off advice if you run your IT in-house. Or even to visit, conduct a data health-check, and if necessary get your Internet connections secure using tools or equipment they know will meet the needs of your business while fulfilling the principles of this White Paper.

Ask them about the questions featured in this article. Ask them if they can help you implement a system which offers regular reporting on user's Web browsing habits. Ask them if they have tools which can ensure malware and other malicious software cannot be downloaded to your network.

Additionally, ensure you implement a suitable policy for your staff. If you do not already have something like the policy contained with the Appendix then seek the advice of a local HR consultant (see later) and ensure you have this aspect of your business covered. It's something you might not think you have time to deal with, but trust me, if you return to the office to find a staff member has sent out an e-mail to your clients saying things that are libellous and you DON'T have such a policy, the consequences would be significant.

Give some thought to what happens if you return to the office and find that some casual lunchtime Web browsing from a staff member had resulted in the infection of a PC, or maybe more ?

Make sure you act before it's too late and you have a court case or a network infection!

 The right Internet usage policy can not only decrease your business's legal liability, but improve employee productivity and your bottom line.

Conclusion

Web filtering has become an essential layer of network security. But unlike other network security solutions such as anti-virus software, content control requires balancing employee needs with that of network security and corporate liability. Filtering is most effective when combined with training, a regular system of usage monitoring, and a clear Acceptable Use Policy. Implementing content control can be straightforward and does not need to take much time. By putting these measures in place, companies greatly decrease the odds of their networks being compromised, reduce their liability, and improve employee productivity.

Appendix

Computer, Email & Internet Acceptable Use Policy

Effective Date: [INSERT DATE]

Revision Date:

To help you do your job, <COMPANY NAME> may give you access to computers, computer files, the email system, and software. You should not password protect any file without authorization. To make sure that all employees follow this policy, we may monitor computer and email usage. All <COMPANY NAME> email is the property of <COMPANY NAME>.

We try hard to have a workplace that is free of harassment and sensitive to the diversity of our employees. Therefore, we do not allow employees to use computers and email in ways that are disruptive, offensive to others, or harmful to morale.

At <COMPANY NAME> you may not display, download, or email sexually explicit images, messages, or cartoons. You also may not use computers or email for ethnic slurs, racial comments, off-colour jokes, or anything that another person might consider to be harassment or disrespectful.

If you know about any violations to this policy, notify your supervisor, the HR Department or any member of management. Employees who violate this policy are subject to disciplinary action, up to and including termination of employment.

Internet Security and Acceptable Use



Use this form to get started today!

<COMPANY NAME> may provide you with Internet access to help you do your job. Internet usage is intended for job-related activities but short, occasional personal use is allowed as long as you keep it within reasonable limits.

All Internet data that is written, sent, or received through our computer systems is part of official <COMPANY NAME> records. That means that we can be legally required to show that information to law enforcement or other parties. Therefore, you should always make sure that the business information contained in Internet email messages and other transmissions is accurate, appropriate, ethical, and legal.

The equipment, services, and technology that you use to access the Internet are the property of <COMPANY NAME>. Therefore, we reserve the right to monitor how you use the Internet. We also reserve the right to find and read any data that you write, send, or receive through our online connections or is stored in our computer systems.

You may not use the Internet to write, send, read, or receive data that contains content that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating, or disruptive to any employee or other person.

Examples of unacceptable content include (but are not limited to) sexual comments or images, racial slurs, gender-specific comments, or other comments or images that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

If you use the Internet in a way that violates the law or <COMPANY NAME> policies, you will be subject to disciplinary action, up to and including termination of employment. You may also be held personally liable for violating this policy.

The following are some examples of prohibited activities that violate this Internet policy:

- Sending or posting discriminatory, harassing, or threatening messages or images
- Using the organization's time and resources for personal gain

- Stealing, using, or disclosing someone else's code or password without authorization
- Copying, pirating, or downloading software and electronic files without permission
- Sending or posting confidential material, trade secrets, or proprietary information outside of the organization
- Violating copyright law
- Failing to observe licensing agreements
- Engaging in unauthorized transactions that may incur a cost to the organization or initiate unwanted Internet services and transmissions
- Sending or posting messages or material that could damage the organization's image or reputation
- Participating in the viewing or exchange of pornography or obscene materials
- Sending or posting messages that defame or slander other individuals
- Attempting to break into the computer system of another organization or person
- Refusing to cooperate with a security investigation
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities
- Using the Internet for political causes or activities, religious activities, or any sort of gambling
- Jeopardizing the security of the organization's electronic communications systems
- Passing off personal views as representing those of the organization
- Sending anonymous email messages
- Engaging in any other illegal activities

Please Note

Should you require this policy in standard Word format for editing purposes, please contact Craig Sharp via info@abussi.co.uk to request the document.

Please Distribute This Article Freely

With Preference To Other Small Businesses Who You Want To Help, By Making Sure They Avoid IT Mistakes Provided that the content and links are left intact, as is, without editing, and that proper credit and attributions are made to the author and his website.

Abussi Ltd

Craig Sharp is a director of Birmingham-based IT company Abussi Ltd.

Mailing Address

1 Victoria Square

Birmingham

West Midlands

B1 1BD

Phone: 0845 862 0200

Email: craig@abussi.co.uk

Web: www.abussi.co.uk

Legal Notice

While attempts have been made to verify the correctness and reliability of the information provided in this publication, the author and publisher do not assume any responsibilities for errors, omissions, or contradictory information contained in this document.

The author and publisher are not liable for any losses or damages whatsoever, including but not limited to loss of business, profits, service, clients, information, or any other pecuniary loss. The information contained in this document is not intended as advice, legal, medical, financial or otherwise, and provided for educational purposes only. You are highly encouraged to seek the advice of a competent professional when applicable.

The reader of this book assumes all responsibility and liability for the use of these materials and information. Craig Sharp, Abussi Ltd and all associated organisations assume no responsibility or liability whatsoever on behalf of the reader of these materials.

Additional Notice and Disclaimers

Any results depicted or implied in this document are atypical of most results. No guarantees, promises or suggestions of any results are made, whether implied or stated. Individual results may vary from those shown, and everything herein is provided on an "at your own risk" basis.

While the author has done his earnest best to make sure you enjoy this report, certain grammatical and typographical errors may still exist. Any such error, or any perceived slight of a specific person or organisation, is purely unintentional. Wherever the neuter is not used, any one gender was chosen for simplicity's sake. This document was created with the hope that the reader finds its content useful and not analysed for the purposes of gender equality, language correctness or writing style.