Introduction

This book is devoted to the most common threats that jeopardise your organisation's data, as well as its productivity, and thus threaten your organisation's financial well-being. To many small businesses, losing their data could mean the end of their existence.

Improperly configured or improperly licensed IT equipment, whether it's PCs and laptops, notebooks or net books, iPads or smart phones, whatever – they're everywhere. It would be a brave – or foolish – Head of IT who would take the stand and swear they were certain (and could prove) all of the IT equipment in their organisation was securely configured, securely used, and licensed completely legitimately. In fact it would be a very brave – or foolish – Head of IT who would swear they even knew (and could prove) what and where all of the IT equipment in their organisation was! And the bigger the organisation, the bigger this challenge becomes.

So, following that logic, you'd think that the smaller an organisation is, the easier it would be to keep all of this IT hardware and software under control. And you'd be right – until you get down to small organisations with few employees, and maybe no-one whose job title has "IT" in it. Especially in the case of small businesses with few employees. Perhaps they have yet to grow to the point where they can afford to hire a dedicated IT person. What tends to happen instead is that whoever understands the most about IT gets to wear the IT hat for part of their working week. They mean well, they're performing a valuable service for their organisation, and they mostly get the job done. And, if they desperately need help, then and only then will firms specialising in IT for small organisations be called in to assist. Because bringing in outside help costs money, and small organisations' very survival depends on them not wasting their resources.

The problem with this situation is that these well-meaning part-timers (I was going to call them amateurs, but that implies a level of condescension I don't feel is appropriate – because they are doing a good job for the most part, and their hearts are in the right place) don't know what they don't know. In other words, they'll make mistakes because they don't know any better, thinking that what works for them at home, or when they're setting up their friends' computers, will work

just fine at work too. And these mistakes could cost their organisation very dearly indeed.

So, if the description above sounds like you, this book is for you.

The business environment of today has changed beyond all recognition from a few short years ago. Now nearly everyone accepts that the digital ways of doing business are quicker, more efficient, cheaper, and lead to higher quality of service. I say nearly everyone because there are still some people who long wistfully for the 'good old days' before computers and the Internet. But for most of us, what has happened is that we like our faster service, our better quality, the personal touch corporations like Amazon give us with their "recommendations for you", and so on. And we have come to expect it. We all want that higher level of service, all the time, from everyone we do business with. The bar has been raised, permanently.

To deliver these business benefits and compete in today's world, it's a necessity for nearly all organisations, large or small, public sector or private, charity or club, to have an 'always on' Internet connection. They will have networked computers, and those computers will share printers, data stores and connectivity to the Internet. Maybe they'll have a bunch of servers too, for things like back-end databases, order processing and fulfilment, web site, invoicing and credit control too – all integrated and automated as far as possible.

To people now leaving school or university and entering the world of work for the first time, there have always been computers – unlike your older employees to whom information technology 'happened'. To your younger employees, IT didn't happen to them, and it isn't a fact of the modern world – it is simply *part* of their world. Like colour TVs or toasters. And the kids still at school have a greater level of functionality on their smart phones than a PC from the 1990s – and EVERYONE has one. And a Bebo or Facebook account.

To which audience am I speaking? The short answer is that this book is aimed very much at *all* ages.

Those of you over 35 probably experienced some of the disruptive but exciting changes that the introduction of IT into every aspect of the workplace brought with it. If this is you, you're probably aware of many of the benefits that IT brings to the party, but also perhaps a little wary

of it – you're not always sure IT can be trusted. As you'll see as you read through this book, you're quite right to be wary, but you can embrace IT and reap the benefits safely once you know how.

To those of you under 35, the real world and the virtual world aren't two different places anymore. You tweet or change your status update when you do something in the real world, or if you see something online that you want to share. You talk to your friends, make friends, watch movies, shop, book train tickets and check the departure boards, all from your phone. Wherever you are. For this generation, with a phone in every pocket, there is no huge distinction between real and virtual. You don't go home, turn on the computer and experience the Internet – you carry it with you and use it all the time. It is part and parcel of being alive, as natural as breathing.

So some of the security measures I am going to suggest you need to adopt are directly opposite to the ease of use you take for granted. But the reality is that the Internet can be a very hostile place, that there are bad guys (and gals) out there, waiting to steal your money, or your identity, or your data. Quite possibly you don't want to acknowledge that the Internet can be so dangerous, but believe me – it can.

So, where I'm pitching this book is between these two extremes. Yes, you do have to be on your guard, but if you take the sensible precautions I'm advising throughout this book then there is no need to become paranoid. And no, you can't pretend that the Internet is not dangerous. You must have some basic security measures in place. And I'm saying to both groups that you need to understand the downside.

You can't pretend that the Internet is not dangerous. You must have some basic security measures in place.

'Always on' connectivity, essential though it is to the delivery of the many benefits of our digital age, brings with it some associated risks. And unfortunately many of these risks are not at all straightforward or obvious to the non-technical person – yet this describes most of today's organisational leaders. It is the chief-level executives who will have to take the responsibility in cases where

their organisation breaks any of the many laws in this area, or suffers an embarrassing (and costly) Data Leakage Incident or similar. The buck stops at the top.

One term I would like to discuss briefly is 'Hacker', because for the most part, the Tips contained in this book are designed to keep your organisation's data out of the hands of hackers. The original meaning of the term was "A good programmer", someone who really knew their stuff. It was a term full of admiration. But since then it has been adopted by the media, and Hollywood in particular, and it is now commonly used to mean "someone who gains unauthorised access to a computer system". Well, I'm no purist, so in the rest of this book I'm going to use hacker or criminal interchangeably. In the minds of most people these days the two mean nearly the same anyway.

As to motives, well the criminal motive is usually money. Other hackers can be motivated by religious beliefs, or they might be animal rights activists, political protesters or peace campaigners and so forth – they've started to be called 'Hacktivists' by the media lately. Yet another group just like the intellectual challenge hacking presents. And then there are youngsters downloading freely-available hacking tools and trying them out just for fun, the so-called Script Kiddies. But that doesn't make them any less dangerous to your systems or your money if they hack their way in.

The likelihood of a given type of attack happening to your organisation will depend on a number of factors, the most important being what your organisation does for a living. For example, if your organisation is in the financial services sector then you probably know everything in this book already. If your organisation is part of national security then you could no doubt teach me a thing or two, and I doubt this book will offer you anything new. However, these days there is no such thing as an organisation that is never targeted, that never receives Spam e-mails. These days all organisations have confidential information in their possession, and they must protect it from all likely threats. If they don't, they risk severe legal and financial penalties, the loss of their livelihood, and the loss of all trust they have built up in their sector.

For its 2010 Annual Security Report, Barracuda Labs polled 637 IT professionals (see the Resources section for details). Only 7% said their organisations had not been hacked at all in 2010, 31% had been hacked between 1 and 5 times, while 42% said their organisations had

been hacked more than 6 times. And a further 20% didn't know whether their organisations had been hacked or not – which probably means you *were* hacked folks, sorry – the hackers were too good for you. And I'm not joking. But I hope for your sake that I'm wrong.

The message I am trying to convey to you here is simple – if your organisation has any computers that connect to the Internet, you can expect at the very least to have your electronic defences probed, and frequently. And if your defences are not good enough in any of the ways I'm going to cover in this book, then you can expect to be hacked. Period.

20% didn't know whether their organisations had been hacked or not – which probably means you were hacked folks, sorry – the hackers were too good for you.

In this book I have attempted to spell out to the average person, of whatever generation, what the risks are when you use computer systems to process data, what the consequences of a Data Leakage Incident can be, and how to reduce the likelihood of them happening to you and your organisation – or eliminate some of the risks entirely. The risks are each discussed individually at first, and then at the end of the book there is a checklist you can use to make sure you have got each risk area covered. Or that you've checked, and are happy a particular risk doesn't apply to your organisation. It's certain that not all of the Tips will apply to every organisation.

This book is intended to be a short introductory guide and summary of the main points of the topics covered, and it's aimed at the non-IT specialist with IT responsibilities, as well as IT personnel. It isn't intended to give you a theoretical grounding in the subjects covered, but it is going to point you at what you should focus on first to make the biggest impact.

Whole libraries full of books have been written about many of the subjects discussed, so don't kid yourself that once you have finished this book you'll know all there is to know about digital-age security. But you will have made a good start in the right direction.

Here's a thought for you before we move on to ***Part 1***. To minimise most of the problems we're about to look at will cost you money, or time, or staff and management resources. Often all three. And if you're not already doing these things it would be very easy to see them as simply extra costs, with no obvious Return On Investment (ROI). So I would suggest you need to take a look at these issues differently. For example, you don't look for the ROI on insurance policies. Things like Public Liability Insurance, Employers Insurance, Auto Insurance, Buildings Insurance – they are all an accepted fact of life when you run any kind of organisation.

So, don't look for an easy ROI for the measures I'm going to share with you, either. They too need to become an accepted fact of life to you when you run any kind of organisation in the present day. And the consequences of not following the Tips in this book can be calamitous.

Am I saying Information Security is just a cost to be borne? Well, it depends. A rigorous approach to Information Security can be (as the UK's Information Commissioner spelled out - see the Resources section for details) a business enabler and a valuable feature of your organisation's offering – there are plenty of opportunities for payback when you follow good Information Security practice. Alternatively it can be seen as a millstone around your organisation's neck, with no discernable ROI.

In the end it comes down to attitude. You or someone in your organisation is going to have to tackle these issues head on and deal with Information Security. And how you view it will very likely determine whether your organisation gains some tactical advantage from it – or just an additional, unwelcome cost centre.

A wise man once said it is much easier to sell a cure than to sell a prevention. They are undoubtedly right, but, in respect of IT security, that mind-set will sooner or later land you in deep, deep trouble.

Each record lost in a Data Leakage Incident costs from $133 up to $249. And Data Leakage Incidents typically involve <u>thousands</u> of records!

Based on April 2010 figures (see the Resources section for details), the Ponemon Institute calculates that each record (in computer speak, a record is all of the data held in a database on one individual customer, such as name, address, date of birth, bank or credit card details, Social Security number and so forth) lost in a Data Leakage Incident costs the organisation that lost it at from $133 (approx. £88) up to $249 (approx. £166) in the US, and from £69 (approx. $103) up to £131 (approx. $197) in the UK. The larger figures for the US reflect both the more penalty-based legal system and also the greater regulatory compliance steps which have to be taken in the US to satisfy the law. And Data Leakage Incidents typically involve *thousands* of records! Be assured, the same level of legal compliance and regulation will come to the EU in the foreseeable future.

I hope you enjoy this book and, more importantly, that it helps you to protect your organisation from some of the most common Information Security headaches. So, buckle up your safety belt and start reading. The Tips coming up will prevent your organisation from making the worst Information Security mistakes.

If you believe something I've written in this book is incorrect or inaccurate then please tell me. And if you like it, please tell all your friends! Either way you can send comments to me:
e-mail **sgibbs@snappytitles.com**.

* * * * * * * * * * * * * <DISCLAIMER>* * * * * * * * * * * * *

Although particular laws may be mentioned, this book is not intended to be (and cannot be taken as) legal advice. This publication can never replace legal advice from your own organisation's legal counsel. And the opinions expressed are those of the author. I'm good, but even I'm not always right!

* * * * * * * * * * * * </DISCLAIMER> ENDS * * * * * * * * * * * *

Right, now the legal bit is out of the way, let's get to it!

Steve Gibbs
March 2011