SECURESTIX

16 Business Destroying Security Flaws Found In Many Companies…

…and how to Avoid them.

A look into IT Security

By Ashton Wood
Director, SecureStix.

Managing Director,
SecureStix Innovations International

Welcome to your guide to securing your company data.

The following information has been gained through many years of experience, discussions, deployments and through speaking with some of the most sought after IT professionals from Australia and around the world.

This document will uncover some key areas of security which many businesses overlook today.

Introduction.

What you are about to read could save you untold worry, concern and loss of business if not addressed.

Before reading on, I want to you to visualise something for me…

Visualise a large fire, tearing through your business, destroying everything in its path – not a nice picture, and probably not a nice way to start this document, but I need to you get present to the total destruction this would cause to your business and your livelihood if this were to happen.

You can most probably rebuild the physical components (eg equipment, machinery etc), you could even re-order all of the core stock you may have had on hand…but how would you replace all of your company data stored on those destroyed computers, your client information, marketing strategies, last seven years' accounting information, emails, proposals…the list goes on.

Now, forget the fire, let's just say someone walked into your office and stole all your computers, backup drives and mailservers (if installed), loaded with all of your emails, proposals, personal files and confidential company data.

The impact on your business from a computer and data perspective would be simular to that of the fire.
In fact it would be worse…as your information was not destroyed and could end up in the hands of your clients, your competitors or even the media!

This e-book will give you a guide on the steps you should consider to protect yourself from the loss or theft of your company data.

Some of the areas outlined in this document may seem very simple, but you would be surprised at how many companies do not have them in place today.

1. Lets start with Physical Security.

Have a look at your office today,
could someone simply walk on in?

If so, could they get past your receptionist?
Would they be challenged?

Are you holding any mission critical files on the receptionists PC?

Do you have any backup drives, removable drives or other laptops etc at or near the reception desk?

Recommendations:

1. Secure your entrance / reception to ensure no-one can get past this point without a pass, a key or an escort by a staff member – if this is not possible, lock down each and every desktop PC, Laptop and portable storage device in the office using the methods below.

2. Secure the computer at reception using brackets and screws to ensure no one can walk in and take this machine away.

3. Move any backup drives to a secure area of the office or into a locked communications cupboard or room.

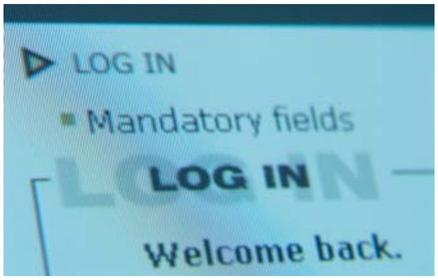
4. Use a “cable lock” to secure your laptop/s which are sitting at desks or workstations – this won’t stop organised crime (a decent set of cable cutters will sever the cable), but will stop the opportunistic thief.

5. Put all laptops out of sight when not in use (eg in a locked drawer)

6. Ensure all staff remove any company information from unsecured USB keys (memory sticks) as these are easy pickings for anyone wanting to get to important information.

   All company information should be stored on secure USB sticks which require fingerprint authentication before allowing access to any of these types of files.

2. Password Security.



Many people find it an inconvenience to enter a password to access their computers, but I highly recommend you adopt this practice.

The password is your first line of defence and this feature should be enabled on all computers within your organisation.

The password should be required when you turn the machine on, and should also be enabled in the screensaver mode.

Recommendations:

7. Turn on password feature on computer startup.
   You can enable this by going to the “start menu”, then selecting “control panel”, then choosing “user accounts” (works with most windows based machines).

8. Enable password prompting on your screensaver and have this activate within 10 minutes of the computer being idle (preferably shorter if you want tighter security) to ensure no unauthorised person/s can access your computer if you’re away from your desk for a period of time.
   You can enable this by right clicking on your desktop, then choose “properties”, then the “screensaver tab”, then tick the “On resume, password protect” box. (works with most windows based machines).

9. Don’t use passwords like your company name, or “password”, “admin” or “administrator”

3. Virus protection / Email fraud

The most damaging viruses are those which you don't even know are there.
"Viruses" come in all shapes and sizes.
Some, called "keyloggers" or "Spyware" log every single Keystroke you press on your keyboard, including bank account numbers, passwords, even the information you type into emails.
All of this information is then sent to the receiver who can use this information to access your accounts, purchase items, or worse, sell this information to other like-minded organised groups.

The more painless types of spyware are those which simply record which websites you are visiting so that companies know your habits and can target products for you.

Email attachments regularly contain viruses, so if you're unsure of the attachment within the email, or of the name of the person who sent you the email, don't open it.

There are also a number of email hoaxes going around which are designed to look like an email from your bank, asking you to click the link and login to your banking environment to verify your details…some even suggest that your details have already been compromised and instruct you to login and change them – never click the links on these types of emails.

Recommendations:

10. Find a good virus protection program immediately.
    Ensure it has regular virus updates, spyware / Trojan protection and preferably Spam email protection as well.
    The best kind also have an inbuilt "firewall" protecting your computer from "attacks" from the outside world.

11. Never click a link in an email from a financial institution, ebay, paypal or any other site which requires your username and password for financial authentication.

    Always type your bank webpage into a new browser window or call your bank or financial institution if you unsure if you should act on an email from them.

4. Wireless Access.

Are you currently running a wireless network?
If so, do you really need it? (eg is there a network point close by which could be used instead?)

Wireless networks are your weakest point of access. If you have, or are considering setting up your own wireless network, be aware that the default setup in most wireless routers configure the connection with absolutely no security – that is, anyone within range can connect to and use your connection to the internet, or worse, access your confidential files!

Did you know that in many capital cities of Australia and around the world you will find "chalk" markings on the footpaths outside buildings?
These chalk markings tell other like-minded people what wireless networks are available and what security (if any) is enabled – so that person sitting on that park bench with their laptop or in that car outside your office could be accessing your wireless network right now…you might want to take a moment right now to look out your window!

If you must run a wireless network, be sure to turn on encryption and go the next step by setting a list of approved devices to connect to your network.

Recommendations:

12. Turn off wireless networks if they are not critical to your business.

13. Turn on encryption if you must use a wireless network.

14. Lock down your wireless network to fixed MAC addresses.

    Each computer has a unique MAC address, it's like its DNA. These are hard coded into the machines and are difficult (not impossible) to replicate.

    Once the wireless connection is established, you can instruct most wireless routers to restrict access to only those chosen MAC addresses.

    This can be a little annoying if you regularly have new users wanting to connect to your wireless network, but is worth the investment in time.

    Once setup, I also recommend you turn off the "broadcast" option in your wireless router - this will ensure that your network is not "advertised" to anyone else within wireless range.

5. USB Keys (Memory Sticks).

Last, but definitely not least, let's look at the humble USB key.
These are a fantastic device as they are portable, can hold ever-increasing amounts of information and are the quick and easy way to store all of your important files in a neat little package.

Most people use these to backup important documents and files.
Many people transfer their current projects to it so they can take them out of the office to work on from the comfort of their homes.
Other people keep all of their personal and secret information on them, like their resume's, personal photos and emails or latest proposal etc.

Although very convenient, the majority of these devices are NOT SECURE in any way.
Should you drop this in the street, or have it stolen from your office, home, car or handbag, all of your information will be instantly available to the finder/thief upon insertion in their computer.
What will they find out about you, your business, your clients or your next big secret product launch?

All unsecured USB keys should be banned immediately.

If USB keys are required in the business, use a USB Stick with a Fingerprint reader built-in to ensure no-one can access your sensitive information.

When closed, the SecureStix Biometric device looks like a stylish USB stick

The SecureStix Biometric device opens to reveal a fingerprint reader, ready to authenticate your fingerprint.

Recommendations:

15. Ban all USB Key (Memory Stick) devices within your company if they do not have Fingerprint recognition technology installed

16. For those employees who must have a USB key, supply them with a secure key which uses fingerprint recognition technology to authenticate the user, available from SecureStix. (www.securestix.com)

I trust you found this e-book useful and hope it gives you some strategies you can put in place to immediately minimise the risk, inconvenience and potential loss of business you would otherwise encounter through the loss or theft of your personal and company confidential information.

If you have found this special report useful and you are not already a member, why not join the "Secure Me" club. www.securestix.com It's completely free of charge and as a member you'll get monthly ideas, tips and strategies that you can use in your business to help you reduce the risk of theft or loss.

Not just that, but you'll also be the first to hear about the newest products as they're being created and will even get to have input on their final design and pricing structure.

Why not tell your friends and colleagues too so that they can share the benefits?

Kind regards,

Ashton Wood
Director, SecureStix
+61 412 281 900
www.securestix.com

PS. This e-book is copyrighted but if you want to forward it to your business colleagues, give it away as a FREE download to people visiting your Website, or as a FREE bonus to your customers, you have my permission.
The only condition is that you do not adjust, alter or change it in any way. It can only be given away exactly as you see here.