Roger’s Cyber Security and Compliance Mini-Guide

A Mini Guide for Small and Medium Business and not for profit organisations.

By Roger Smith
Managed Service Provider and Cyber Security Coach

R & I ICT Consulting Services Pty Ltd
LinkedIn profile: http://www.linkedin.com/pub/roger-smith/1/9b4/383

PLEASE FORWARD TO OTHERS

This is a FREE Guide. You are welcome to forward this guide or the webpage link http://rniconsulting.com.au/home/free-stuff/free-reports/free-report-rogers-cyber-security-compliance-mini-guide/ to your clients and contacts.

For Publishers

Please feel free to use the content in this guide for publishing in magazines, newsletters, etc.

Please do not change the substance of the content. Simply cite the author, publication title and website.

The abbreviated content in this document is taken in part from a number of publications by this author including the Book “The CEO’s Guide to Cyber Security”.

R & I ICT Consulting Services Pty Ltd
PO Box 368
Kippax ACT 2615
AUSTRALIA

Keep in touch! For new articles and guides
Email: Newsletter@rniconsulting.com.au
Downloads: www.rniconsulting.com.au, www.smesecurityframework.com.au
Twitter: Follow @smesecurity
Linkedin: Connect at http://www.linkedin.com/pub/roger-smith/1/9b4/383
Google Plus: Circle Here
https://plus.google.com/u/0/b/104899476259019742957/104899476259019742957/posts/p/pub

Subscribe: Free subscription at www.rniconsulting.com.au.

NOTE: The information in this guide is of a general nature only. When making decisions about your business it is strongly recommended that you seek qualified advice tailored to your particular needs and business situation.

TABLE OF CONTENTS

WHY PROTECT YOUR BUSINESS FROM CYBER CRIMINALS?

It doesn't matter what day of the week or week in the year there is always something about cyber security and Cyber Crime in the news. With the US Congress discussing new cyber security bills constantly, it is something that is relatively hard to miss.

The problem is that regulation will only go part of the way. Small and medium business and not for profit organisations need to focus their own resources on resolving the problem of data security. All this talk may seem irrelevant and not important to SMB's. This is definitely wrong, a false sense of security.

These are five reasons that SME's should be concerned about cyber security and protection of their business information.

1. Smaller organisations are better and easier targets.

This one is relatively easy to prove. Symantec keeps record of this and in the last 18 months organisations fewer than 500 staff have the highest rate of compromise @ 40%. Most of the reasons are mainly due to their size. Small organisations cannot afford the technology, or staff to focus just on business and data security. They also have minimal resources to maintain a secure business environment.

SME are not only targeted by eternal groups, individuals and automated attacks they are also attacked by disgruntled and ex-employees.

2. A security breach for an SMB can potentially be business ending.

The loss of a business critical information, intellectual property, credit card information or client and staff information can be

crippling. If this loss of information is combined with no disaster recovery, business continuity and backup components then the information is not only lost or in the wrong hands but you may never get it back again.

3. Control access to the information internally.

Most small organisations are a trusting lot and consider all employees as trustworthy. All staff logging on as the same user with the same password is a very dangerous situation for SME's. If the SME does not audit system and data access then when something does go missing there is no way of defining the parameters of the loss. This is further compounded when all users are using the same credentials.

This includes access to databases, system access from administrators and keeping track of the data going in and out of the organisation.

4. Protect your reputation.

Have you ever been in the position where you do not want to do business with a company because of what you have heard, either professionally or in passing. Now turn it around to YOUR reputation. If it is tarnished by a security breach, will it affect how your clients do business with you.

5. Protect all of your data including your external contractors.

This can have devastating effects on small organisations in regards to going to the next level of business. A joint venture type of business environment could fall apart relatively quickly if one of the partners are compromised.

Business security and your business reputation are critical to how you do business. If you do not invest in your business security infrastructure then you could be in trouble. The level

of protection that you need will not be in place when you need it. The security investment that you make is not only focused on protection, it should also include the management, resilience and compliance requirements of the business

HOW CAN YOU PROTECT YOUR BUSINESS?

There is no overall and available **How-to** that can be used to bring SMB's up to a consistently higher level of cyber security and resilience. Using a particular product, complying with a particular rule or creating cyber resilience are only facets of the business security profile. Proper and sustainable business security is a combination of all three.

SMB's should take a holistic attitude to protecting their data from both internal and external threats. It is no longer a case of using one product to achieve the total protection that the larger security companies are pushing –

"*Use our -- insert technology here -- and you will be forever protected"*

What a load of BULL.

The newest cloud product, network managements system or user based security widget is not going to create a complete cyber security environment for any business let alone SMB organisations with limited money and expertise. The introduction of a single component or widget will cover a small percentage of the total protection of the required business environment.

Don't get me wrong; in its place the purchased widget will probably do the required job. It is not where business security should stop. Once the widget is in the business environment it has to be used within the holistic framework as a component of the whole.

SMB's need a system that once applied will lift the business security to a higher level, where the bad guys will go after someone else - hopefully a competitor.

SMB’s need protection from:

- ✓ Drive by attacks, (automatically downloaded from infected websites)
- ✓ Internal user problems - including stupidity
- ✓ Opportunistic attacks – Malware, spyware and virus attacks
- ✓ As well as sustained and persistent ones that are directed specifically at the organisation.

This security system or framework also needs to be able to adapt and change to meet emerging security requirements, fight emerging security threats, incorporate new technology and new compliance requirements as they become critical for a business.

You put a complete security systems in place to protect your intellectual property, your staff, your clients and your overall business from attacks. We are not only talking about the outside cyber criminals and automated attacks, what about the disgruntled employee or overlooked IT staff member, they are just as bigger threat to the business as anyone else.

WHERE DO YOU START?

There is no cheap way of securing your organisation, but there are ways to use available systems that will increase your awareness and protection without excessive costs. There are four areas where SMB's need to focus.

Business technology

This is the hardware and software that a business purchases to either protect the business or for the business to use to do "business". Anything to do with computers, laptops, servers, firewall, operating systems, applications, cloud or smart appliances (phones and tablets) is managed through this component. The introduction of one type of technology could cover a number of requirements in the framework but not all of them.

So let's start with decent technology -

- ✓ Use a good firewall, VPN and wireless system
- ✓ Use good operating systems,
- ✓ Use good applications.
- ✓ Protect yourself from SPAM, malware, spyware and worms
- ✓ Use best practice where possible
- ✓ Update everything when it comes out
- ✓ Don't go to or download from dubious sites, in most situations free is bad.

Command, control and management

No matter what part of the business you are looking at there has to be some level of control and management, security is no different. You have to put security systems in place around your business requirements, the problem is that the business

still needs to function as well as protect the data and information that it uses to do business. This is a fine line.

So put good management practices in place

- ✓ Use policies, procedures and processes to tighten up what people do in your business
- ✓ Train you staff
- ✓ Audit and monitor systems
- ✓ Create a comprehensive reporting environment

Adaptability

Like nature, all business needs to adapt to change otherwise they will perish. Some large businesses have changed in such a way that they no longer resemble what they started off as. The largest component of the adaptability component is resilience. The ability to see opportunities and react in a beneficial way is important for any business but it is critical for an SMB.

So get adaptable

- ✓ Have a good backup and restore system
- ✓ Have a business continuity and disaster recovery plan
- ✓ Do a risk assessment
- ✓ Build a winning business culture
- ✓ Build in resilience

Compliance

The worst component of SMB security is the ability for the organisation to meet the compliance requirements. Everyone hates an audit, one that can close down your business is even worse. In a security framework the other three components are leading the organisation towards a compliant environment. The compliance component is no longer a tick in the box type problem, it is the way the business IS. By all means, tick the

boxes on a compliance audit but it is so much better and easier in the long run to live within the compliance mantra.

Get externally audited and compliant and certified in the above areas. This will help make sure that you meet all of the compliance requirements

FINALLY

These are just a few ideas when it comes to protecting your business from the bad guys. One final word, talk to an ethical hacker and get a penetration test done on your business. This will define how secure you really are from the Internet.

The bad guys may still win but by using better protection than they are expecting they will probably move on to easier targets, and it is so much better if the bad guys rob another bank than yours isn't it!!!!

Yes security is important, if not critical for SMB's. The more organisations go digital, the more security will become paramount as a business driver. Security is not one dimensional, you are no longer just protecting your business but business and data security also means protecting your most important asset - your clients and customers.