CARE MANAGED IT

LEGAL AND COMPLIANCE

By Roger Smith

Managed Service Provider, Cyber Security Coach and Virtual Chief Information Security Officer

CareMIT 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 <<location URL>> 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 several publications by this author and others including the Book "The CEO's Guide to Cyber Security" and the National Institute of Standards and Technology (NIST) department in the USA

Care MIT Pty Ltd
3/116 – 118 Wollongong Street,
Fyshwick, ACT 2906
AUSTRALIA

KEEP IN TOUCH! FOR NEW ARTICLES AND GUIDES

Email: support@caremit.com.au

Downloads: https://caremit.com.au/downloads

Twitter: Follow @smesecurity

Linkedin: Connect at http://www.linkedin.com/pub/roger-smith/1/9b4/383

Subscribe: Free subscription at https://caremit.com.au/newsletters

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 needs and business situation.

CONTENTS

INTRODUCTION

When it comes to protecting organisations, the biggest vulnerability is the staff.

In this error of persistent cyber threats, an organisation can be secured only with active participation from everybody.

> **Cyber security.**
>
> Described as measures taken to protect a computer or computer system against unauthorised access or attack.
>
> **Webster's dictionary.**

Unfortunately, many organisations, small and medium enterprises, not-for-profit organisations and charities limit the security responsibilities to the designated security personnel that are perceived to be the people who would understand the security functions.

Effective security must be enterprise wide, involve everybody in fulfilling security capabilities and to be aware of the requirements to protect the data and information.

> **Business Security**
>
> Using a system that includes policy, process, procedures, plans, standards, detection, education, technology and risk management to protect a company
>
> **Roger Smith**

Everybody with an organisation from the newest employee to the executive suite holds the capability and the power to not only help the organisation but to also harm it severely. Get your

This guide outlines what each of us should do to protect our organisations based on the type of work we all do.

BENEFITS OF THIS GUIDE

This guide breaks down your role and job requirements and what functions you need to address within that role.

All roles both technical and non-technical have a requirement to secure critical information and systems.

This guide provides essential must do guidance in simple language.

This guide turns our greatest vulnerability, its people, into an asset.

WHY THIS GUIDE IS NEEDED.

Most organisations and executives within organisations have a common misunderstanding that cyber threats are technological problems and must be addressed with technological solutions.

From all the information on the Internet consistently shows that employees are the greatest vulnerability to any organisation.

No matter how hard or robust the cyber security policies that have been introduced by executive management the organisation cannot be secured without first securing the capabilities and understanding of the employees.

If you use the example of public health. Active participation by everybody is required. We are all educated to encourage and exercise good hygiene such as washing hands and seeking with preventative care through immunisation. Even children have been indoctrinated into hand washing sneezing into elbows and so forth. Well-trained professionals restrict the movement of disease through good hygiene. So for good cyber hygiene we all need to take appropriate care to protect the organisation.

A further misconception is that organisations just need more technological savvy or technology to secure an organisation. These people are important to implement essential technological safeguards and for ongoing security operations.

The largest attack surface within a business structure is always going to be you, the people you work with and the people you interact with.

Therefore, cyber security is everyone's job.

WHO CAN USE THIS GUIDE?

This guide is intended for every kind of organisation from large government agencies to not-for-profit organisations and basic SMEs. All businesses have a fundamental requirement to generate revenue, communicate with external customers and stakeholders, deliver products and services, lead people and manage financial and legal matters. All of these require some type of computer system.

Each of these areas routinely expose the business to a variety of cyber related business risks.

To reduce these new digital risks each person in each business function must be involved in securing the organisation, understanding their role in the organisation and take individual responsibility for mitigating the risks associated with the digital environment.

In the following pages your find practical information to action in accordance with your business function.

Many of these tasks are simple. In fact, they may seem so simple that they may seem inconsequential.

This guide reflects proven best practice developed by security experts working within the digital environment of large numbers of organisations.

The cyber security, digital protection and risk management of your organisation depends on you.

This is what you can do:

HOW TO USE THIS GUIDE.

This guide is broken down into business functions, those essential activities which organisations must perform to at least some extent to make the organisation work correctly.

Each represents work that can be performed by a number of people in that role or in that roles environment.

They are intended for full-time employees, part-time hires, leaders at all levels and for those people who perform tasks at that business function.

The goal is to build a cyber secure workforce with each person doing their part to make the organisation more secure.

The business functions are represented in seven categories.

- Leadership planning and governance
- sales marketing and communications.
- Facilities physical systems and operations.
- Finance and administration.
- Human resources.
- Legal and compliance.
- Information technology.

Each function within an organisation can use this guide as a standalone reference for that particular function. Because of this some functionality will appear in multiple sections.

The information in this guide is not intended to replace your organisation security policies, rather it provides a supplemental quick reference of actions that anybody can perform to increase the businesses cyber resilience.

BUILDING A CYBER SECURE OR CULTURE

your organisation's culture is critical to establishing a successful business security posture.

The businesses culture must emphasise, reinforce and drive behaviour towards a secure digital environment.

The better the business security culture the more resilient the organisation and the workforce within that organisation.

MINDSET.

A critical component of the organisation's culture is the mindset of all staff.

When we build awareness into the business culture, we increase our ability to address business security risks.

Every organisation is at risk no matter the size of the organisation or the management style of the executives.

Mindset will drive appropriate behaviours at the individual level, contributing to better business security within the organisation.

LEADERSHIP.

The business leaders and executives set the tone for the business.

Leadership or the lack of leadership is one of the most important factors in influencing awareness and changing the mindset of the business.

Leaders must embrace cyber security education, awareness and best practices.

The executives of every organisation must support security investments and champion cyber security from a risk management perspective.

A requirement for a deep technical knowledge for the leaders is not needed, but they should model the business security profile based on sound guidelines and best practice.

Leadership involvement is critical for a secure business environment.

TRAINING AND AWARENESS.

Employee awareness training is the next step to implementing a secure business environment.

These programs build an understanding of business risk and, most importantly, provide specific steps in mitigating those risks..

Training and awareness programs come in many forms. Training can be online, off-line, individual or as part of a group training session.

Training and awareness are required to reduce the impact of social engineering or the manipulation of all users. Social engineering is used to spread exploits by unsuspecting employees and is an increasing risk to every company.

A key element to all training is to increase your staff's awareness to socially engineered exploits.

No program however will lead to a sustained 100% success rate against human-based attacks. They can reduce the volume and impact of the attacks because of their awareness.

Further ways to build cyber secure culture is through internal awareness programs. Posters, regular emails, newsletters, contests and or prizes have been found to increase and generate "buzz".

Training and awareness programs should be a year-round activity not just a one-off process.

PERFORMANCE MANAGEMENT.

Incentives and disincentives can have a profound impact on your staff's behaviour.

For real change to occur in business security preparedness, individual performance goals must align with the business goals.

Performance goals for business security can include.

- Completion of required training.
- Improved responses to fishing exercises.
- Compliance with policies.
- And a reduction in risky online behaviour.

Most organisations already have financial and operational metrics, security metrics should now be included as well.

TECHNICAL AND POLICY REINFORCEMENT.

Technological controls that enforce human behaviour can be implemented to increase business security cultures. Security controls such as.

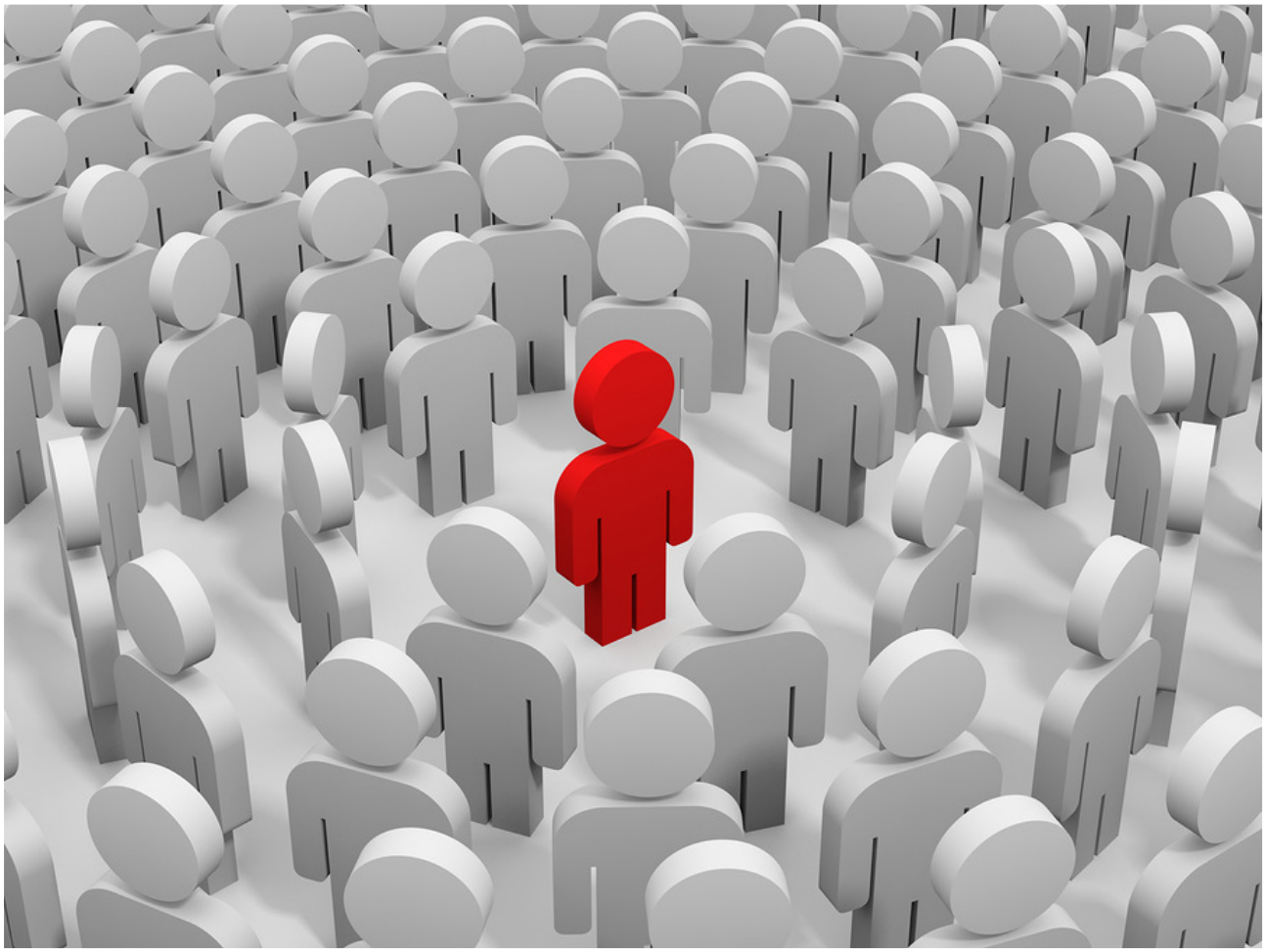
- Password policies.
- Two factor authentications.
- Mobile device management.

Policies at the business level can also drive the implementation of controls by outlining the negative consequences of non-compliance.

There are many ways that this guide can be implemented within the unique culture of every organisation.

These instructions should form the basis for developing a business security culture by increasing awareness and fostering the right mindset.

With the sound business security culture in place each business function can focus on its own contribution to protect the business.



LEGAL AND COMPLIANCE.

WHAT LEGAL AND COMPLIANCE DOES.

If your role in the business is to mitigate and respond to legal risks and compliance requirements this section applies to you.

You do this in a large part by ensuring that the organisation remains compliant with the numerous laws, regulations and standards that apply to the business as well as the industry.

Ensuring compliance with laws, regulations and standards, mitigating risks and addressing legal matters.

You are a close advisor to senior leaders and help to set policies and priorities that balance the organisations primary purpose with the risks to which it may be exposed.

You are highly responsive to legal threats and may become the focal point from outside the organisation.

You matter to the organisation because you ensure that it remains in good standing with laws, regulations and standards. This allows the organisation to focus on core capabilities.

THE ROLE OF LEGAL AND COMPLIANCE IN BUSINESS SECURITY IS ALL ABOUT.

1. Minimising liabilities associated with the business security posture of the organisation.
2. Ensuring compliance with cyber security laws, regulations and standards.
3. Addressing the legal implications and impact of incidents when they arise.

WHAT LEGAL AND COMPLIANCE PROFESSIONALS SHOULD DO.

- Understand the legal implications of business security in order to enable sound risk mitigation.
  - Engage with credible third-party is to learn about cyber security and law. This includes professional associations, industry groups, consultants and educators.
  - Remain current on emerging regulations and standards.
- Implement an effective compliance program for the business.
  - Assess the organisation's exposure to laws, regulations and industry standards to ensure appropriate coverage.
  - Establish and enforce information classification and assess processes.
  - Leveraging existing best practices for compliance and enforcement.
  - Ensure that third-party and supply chain organisations adhere to cyber security policies through contractual and service level agreements.
- Actively participate in the enterprise risk management process to mitigate risks in a Hellenistic manner.
  - Implement measures to mitigate risks introduced by partners, vendor's and suppliers.
  - Actively support the organisation's incident response during a cyber event including taking appropriate steps to preserve legal privilege as much as possible.
- Conduct post-incident legal enforcement engagement, vendor notification and public notification as required.
- Protect sensitive information concerning employees recruiting, performance, compensation and benefits.
  - Share only necessary information.
  - Ensure the information is destroyed in accordance with compliance requirements and data protection requirements.
  - Use encryption, passwords and other methods to secure files when transferring outside the organisation. Especially for recruiters.
- Ensure the accounts of terminated employees are closed promptly.
  - Immediately notify IT or managed service provider of pending and actual terminations.

- Update directories, internal access, permissions and external access to restrict access to people no longer employed by the organisation.
- Update HR records accordingly.

WHAT WE ALL SHOULD DO.

- Ensure that all operating systems and applications are at their most current and most secure by enabling automatic updates based on the vendor's requirements.
- When working from home or an environment you have no control over apply the following best practice.
  - Change your wireless password, SSID and limit access to the system.
  - Maximise encryption levels on your Wi-Fi system.
  - Increase privacy settings on browsers.
  - Use virtual private networks to access the corporate network.
  - For additional security use an encrypted browser.
  - Protect personal email accounts through encrypted email.
  - Do not enter sensitive information on public computers such as business centres libraries an Internet café's.
  - Do not access public Wi-Fi without a pass phrase.
  - Use a personal hotspot for Internet access.
  - If you are travelling to regions where there is questionable data security or excessive surveillance use a disposable phone.
  - Physically protect your computer from theft and unauthorised access.

YOU SOCIAL MEDIA. WISELY.

- Use strong privacy settings on all social media platforms.
- Don't share personal information on business accounts.
- Don't share business information on personal accounts.

DOING THE RIGHT THINGS.

in the forensic process, after a cyber event, the process used is focuses on finding patient zero. This is a term adopted from medical forensics and is used to identify the person or group of people that was the entry point for malicious exploitation into the information technology and digital environment.

While multilayered security protection strategies are important the organisation is still relying on individuals to do the right thing.

Anybody and everybody within a business no matter the level of expertise, capability or business requirement have damaged the organisation's brand and reputation or even lost their jobs when a cyber event has occurred.

The obvious question for personnel in these businesses is what should I do to avoid becoming patients zero?.

The following are guides for all individuals. Regardless of business function everybody who is connected to the digital world needs to avoid becoming "patient zero"

What everybody should do in a general straightforward sense is to to to become more cyber aware and exercise better cyber hygiene to reduce the risks of a cyber event.

In the context of business security and the digital business environment, all businesses want to create a robust cyber security culture. To do that the business must implement good cyber security practices to mitigate their critical cyber security risks.

More importantly everyone must contribute to the organisation security. To be successful in this area this cannot be a one-time awareness of training event but a continuous effort to make everybody aware of current cyber related risks and the practice the organisation expects each person will perform.

In general, every individual within an organisation should be performing the following common tasks.

- Exercise caution when using information systems. If you are unsure or sense you may be doing something good risky seek guidance from responsible individuals.
- Fully understand your role in taking personal responsibility for knowing how your organisation addresses the events of a cyber security risk.
- Be willing to learn since technology is continually evolving.
- No how to handle, control, store, transfer and dispose of information in your organisation.
- Protect your assets by physically safeguarding your computer Mobile device and non-electrical information.
- Follow your organisation security procedures, policies, processes for all facilities and prevent an are theorised access via social engineering tricks.
- Use the best authentication capabilities your organisation offers for controlling access to computers, mobile devices and the information services and the applications you use.
- Use encryption for information in transit and at rest.
- If you work from home secure your home devices and connections.
- If you travel know your organisation want you to secure your connections back to the organisation through public networks.
- No your organisation's policies and practices for using personal devices for work.
- Now your organisation security incident reporting policy and their contacts.
- Takes control of your own cyber security and safety don't assume that hardware and software providers will do it for you.