CARE
MANAGED IT

https://virtual-ciso.com.au/everyones-job/

By Roger Smith

Managed Service Provider and Cyber Security Coach

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”

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

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 needs and business situation.

CONTENTS

Virtual Chief Information Security Officer
"Business security is my problem!"

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.

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.

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.

Cyber security.

Described as measures taken to protect a computer or computer system against unauthorised access or attack.

Webster's dictionary.

Business Security

Using a system that includes policy, process, procedures, plans, standards, detection, education, technology and risk management to protect a company

Roger Smith

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.

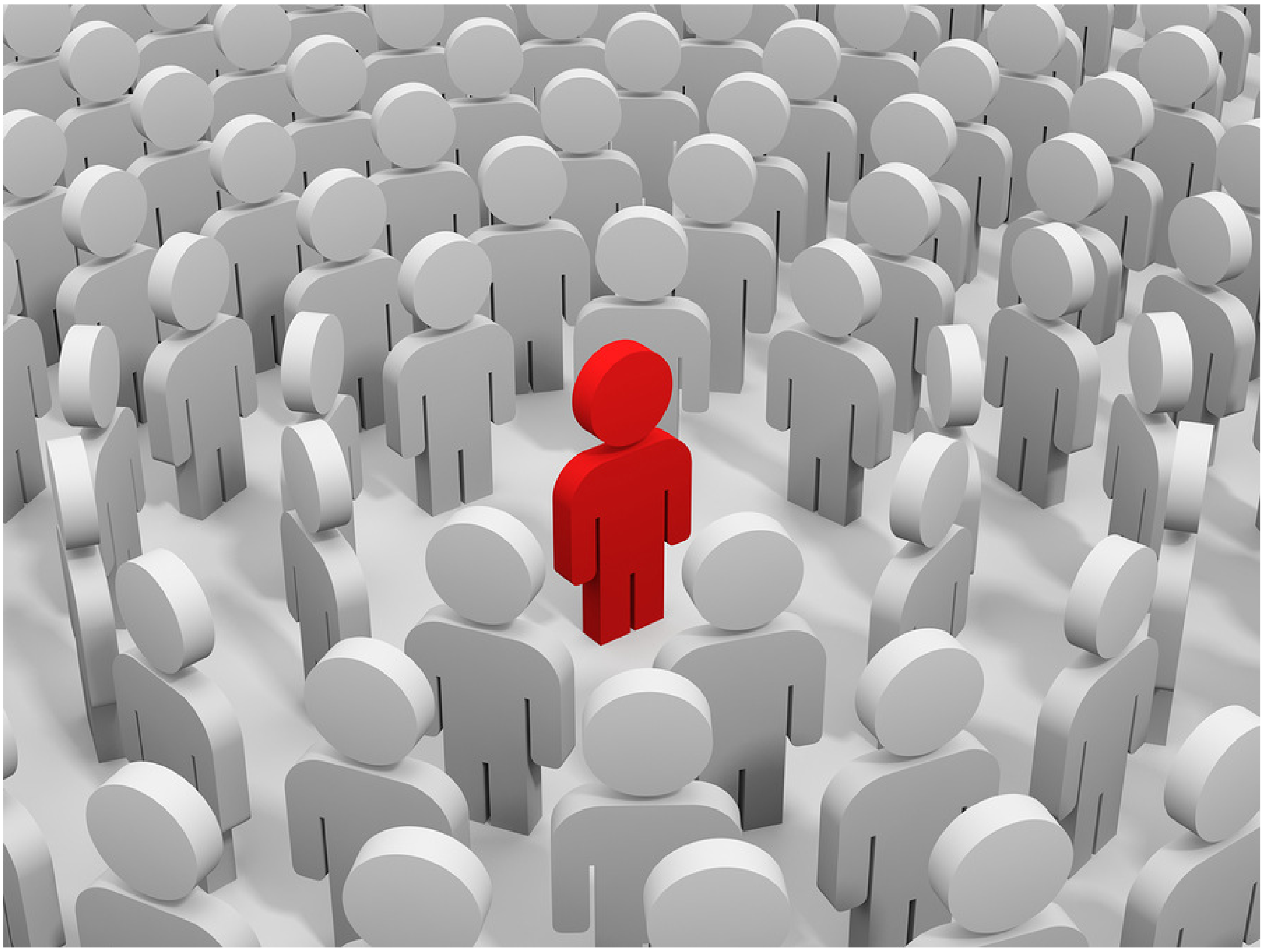
- Password policies.
- Two factor authentications.
- Mobile device management.

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.



LEADERSHIP, PLANNING AND GOVERNANCE.

WHAT DOES LEADERSHIP, PLANNING AND GOVERNANCE DO.

This section applies to you if you are responsible for the overall strategic direction, maintaining controls and mitigating risks of the business.

The c level executives are the most senior leaders within an organisation.

This area is responsible for overall direction, establishing priorities, maintaining influence and mitigating risks.

This section applies to people involved in board proceedings, contributing to senior level management all managing complex agencies and organisations.

You could also be the owner operator of a small business or franchise.

This area has a common role within all organisations and that is the final decision, the buck stops with you.

You will play a critical role in establishing priorities and ensuring adherence to those requirements. At the same time addressing business risks is a critical component of your role within the organisation.

You are the direction and the cohesion for everybody within the organisation.

THE ROLE OF LEADERSHIP, PLANNING AND GOVERNANCE IN BUSINESS SECURITY IS ALL ABOUT.

1. Managing and mitigating overall cyber -related business risks.
2. Establish effective governance controls.
3. Prioritising, managing and monitoring business security resources.
4. Safeguarding sensitive and private information that is used to make business decisions.
5. Creating a business security culture within the organisation.

WHAT LEADERSHIP, PLANNING AND GOVERNANCE PROFESSIONALS SHOULD DO.

➢ Understand business security basics and best practices well enough to enable sound decision-making capabilities.

- Establishing reporting processes for cyber and business risks.
- Engage with third-party to learn about business risks and what other organisations are doing or using to mitigate those risks.
- Commission risk assessments for the company.
- Direct the implementation of best practices, frameworks maintained by external entities. (National Institute of standards and technology, Centre for Internet Security, Australian cyber security centre.)

➢ Include all digital risks in the enterprises risk management process.

- Avoid treating cyber risks as a separate entity only addressed by technologists.
- Understand the impact of a cyber incident on the organisation.
- Incorporate risks introduced from supply chains, partners and suppliers.
- Use tabletop exercises and decision-making drills to respond to disasters and cyber events.

  - Prioritise cyber -related risks to ensure appropriate attention and effort is committed to mitigating those risks.
- ➢ Develop and maintain organisations information security policies and standards.
  - Ensure that information security policies and privacy requirements are included in risk assessment, regulations and standards of the organisation.
  - Ensure organisational security policies up appropriately implemented and communicated to all members of the company.
  - Be aware of relevant data protection and privacy requirements and legislation to ensure that your organisation stays in compliance. (General data protection regulations, health insurance portability and accountability act, Federal information Security Management act, Freedom of information act, SaBains-OxLey (SOX).
  - Have a regular review of all policies
  - promote and develop effective cross functional teams to accomplish business security within the organisation.
- ➢ Fund business security and resources based on priority and request.
  - Digital assets cannot be protected without human and technical resources. A commitment of resources must be aligned with cohesive business security strategies. Plan for your future needs.
- ➢ Protect sensitive strategic, financial, legal and risk information.
  - Share only necessary information both within and outside the organisation.
  - Ensure that information is retained or destroyed in compliance with data protect retention policies and external regulations.
  - Use strong encryption, strong passwords and other ways to secure files when you transfer them to others.
- ➢ Protect access to online file sharing or decision applications by applying best practices such as.
  - Strong pass raises.
  - Unique pass raises for each critical account.
  - Multifactor authentication.

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.

USE 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.

SALES, MARKETING AND COMMUNICATIONS.

WHAT'S SALES, MARKETING AND COMMUNICATIONS DOES.

If you are interacting with customers, clients, donors or citizens this area applies to you.

Sales, marketing and communication professionals are those who engage perspective an existing customer to drive awareness of products and services, stimulate interest and generate revenue through sales or other means.

> *Raising awareness, communicating, generating revenue and interaction with customers.*

You may also be involved in public and media communications.

You are the communications messenger of the organisation, carrying news of the good things you provide to those who need to know and responding to current events.

You are often the most visible, outward facing people in the organisation.

You matter to the organisation because without you ideas products and services would not be sold.

THE ROLE OF SALES, MARKETING AND COMMUNICATIONS IN CYBER SECURITY IS ALL ABOUT.

1. Protecting the company's brand, reputation and trust to the general public, customers, partners and vendors.
2. Preventing and limiting information lost as you interact with the outside world.
3. Reducing risks to the business systems presented by remote work telecommuting and travel.

WHAT'S SALES, MARKETING AND COMMUNICATIONS PROFESSIONALS SHOULD DO.

- ➢ Communicate the importance of cyber security matters to your stakeholders.
  - Access reputable sources to develop well-rounded understanding of how information and systems fit into the ECO system of the business.
  - Inventory the types of information under the care of the organisation and consider potential impacts of data compromise from customers, staff and partners.
  - Understand the potential impact of a cyber incident including customer trust and competitive advantage.
- ➢ Develop a communications plan in the event of a cyber event.
  - Participate in internal incident response team planning.
  - Become familiar with an incident response.
  - Participate in tabletop exercises as the communications component to keep external stakeholders involved.
  - Create a communications plan consistent with regular three requirements, legal considerations, industry best practices and promises made to external stakeholders
- ➢ Protect shared files and folders.
  - Use encryption, passwords, to fetch with indication, single use access to secure files when transferring them between customers, vendor's, prospects and stakeholders.
- ➢ Protect access to cloud-based and terrestrial based customer relationship management software by using best practice.
  - Use strong past phrases.
  - Unique past phrases for every account.
  - Multifactor authentication/2 factor authentication.
  - Biometrics.
  - Restrict access levels to required needs.
  - Manage obsolescent access to the database when involvement with the company is no longer available.

- Protect customer information in quotes, purchase orders, invoices, payments and presentations.
  - Share only necessary information.
  - Ensure all information is destroyed in accordance with the organisations retention policies.
- Bring customers cyber concerns back into the organisation.
  - Be aware of the implications of conducting business in a foreign jurisdiction with totally different compliance and governance regulations.
  - Be aware of sovereignty requirements of data held in data centres.

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.

FACILITIES, PHYSICAL SYSTEMS AND OPERATIONS.

WHAT DOES FACILITIES, PHYSICAL SYSTEMS AND OPERATIONS DO?

What facilities, physical systems and operations does.

If you are designing and delivering the products and services created by your business, you are part of the operations environment.

The wide variety of products and services delivered by all businesses to all consumers means there is a diverse range of roles that this area covers.

Designing and delivering products and services, managing operations and maintaining the physical environment.

You matter to the business because successful delivered development and delivery of products and services depends on you. The organisation would cease to function without the capabilities you provide and the primary purpose or core business would go unfulfilled.

Your role in the organisation is crucial to maintaining a competitive advantage over your competition.

THE ROLE OF FACILITIES, PHYSICAL SYSTEMS AND OPERATIONS IN CYBER SECURITY IS ALL ABOUT.

1. Protecting the uniqueness of your products and services.
2. Protection of intellectual property and trade secrets.
3. Securing physical systems from compromised dues to external hazards including physical and digital issues.
4. Integrating digital security with physical security and access to physical systems.

WHAT FACILITIES, PHYSICAL SYSTEMS AND OPERATIONS PROFESSIONALS SHOULD DO.

- Identify digital risks to physical systems and implement resilient components.
  - Engage IT and OT stakeholders to ensure systems are secure.
  - Engage with trusted third parties to develop mitigations for cyber risks in the physical environment.
  - Perform a comprehensive assessment of the physical environment to ensure vulnerabilities and weakness have been addressed.
- Ensure appropriate physical security controls are implemented within the office environment.
- Develop a comprehensive plan to improve the security of control systems (IOT and SCADA)
- Leveraged a cyber security best practice framework to ensure security of control systems is in place
  - In corporate business security measures into safety programs.
  - Ensure employee training includes awareness of business risks and risks to the physical environment.
  - Leveraged the safety program as another way of increasing awareness and fostering a business security culture.
  - Partner with the IT department or manage service provider to develop a system for guests who access the physical environment including limited direct access, access to restricted Wi-Fi networks, access to data held on management systems and reducing access to the physical network.
- Protect the intellectual property and trade secrets of the organisation.
  - Use encryption, passwords and other methods to secure files when transferring them to and previous sections customers and partners.
  - Share only the information that is necessary.
  - Ensure that all sensitive information is destroyed in accordance with compliance and governance systems.

  - Prevent remote access to systems unless absolutely necessary or security components are in place.
- Consider security risks and mitigations in the supply chain.
  - Ensure security controls and systems are embedded within products where necessary.
  - Ensure suppliers and supply chain organisations adhered to security best practices.
- Protect access to information repositories.
  - Apply recommended best practice.
  - Implement strong past phrases.
  - Use unique past phrases for each crucial and critical account.
  - Always deploy multifactor authentication.

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.

USE 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.

FINANCE AND ADMINISTRATION.

WHAT FINANCE AND ADMINISTRATION DOES?

Providing planning, forecasting, accounting, transactional and administrative support to all functions within the organisation

If you are involved in managing the business's finances, from planning and budgeting to accounting and processing then this section applies to you.

You are responsible for ensuring that each part of the organisation has the ability to pay for goods and services, operate within a budget, track revenues and expenditures and conduct the business with external entities.

You may also provide administrative support to the planning and governance function or manage office operations.

This function also includes full-time roles in this area and applies to executives' managers and associates who handle finances and administrative matters.

In many cases the finance and administration function include enterprise risk management, internal audit, compliance requirements and governance.

Your ability to maintain financial health, perform essential transactions, manage business risks and support the planning and governance functions means your role is vital to the business.

THE ROLE OF FINANCE AND ADMINISTRATION IN BUSINESS SECURITY IS ALL ABOUT.

1. Integrating cyber risks into the businesses risk management process.
2. Resourcing business security initiatives consistent with security strategy and balanced with other IT requirements.
3. Maintaining the confidentiality and integrity of sensitive information relating to financial welfare of the business.

WHAT FINANCE AND ADMINISTRATOR PROFESSIONAL SHOULD DO.

- Ensure that cyber risks are integrated into the enterprise risk management system.
  - Identify digital related risks to the enterprise early in the merest management process not as a separate activity or late addition.
  - Understand the many different business effects of a cyber event which range from business disruption and loss of credibility to legal liability and physical damage.
- Provide sufficient funding to enable the success of the organisations business security strategy.
  - Reference the businesses security strategy and external best practice framework to prioritise investments.
  - Work with business security leaders to understand how their resource requests align with the strategy of the organisation. Differentiate between the must haves and the nice to haves.
  - Develop a complete view of business security -related spending which is often spread across multiple function areas and budget allocations.
- Collaborate with other business functions on a plan for business continuity and disaster recovery spending.
  - In the event of a cyber event incident response plan should also incorporate how to purchase needed equipment announces services.
  - Vendor's and contractors should already be vetted and in place if such an incident should occur.
  - Contingency plans, business continuity and disaster recovery requirements for the loss of the financial system to ensure minimal disruption.
  - Cyber risk insurance to offset the financial impact of a cyber event.

        - Ensure that all plans include external financial requirements for instance credit monitoring systems.
- Work with legal and compliance and information technology to ensure that contracted third parties include effective oversight of breach systems on their side.
- Define the appropriate balance of resource allocation between running the business and improving the business.
    - Ensure that all run the business and improve the business requirements do not expose the organisation to new risks.
    - Improvement to IT operations not only can improve security and compliance but they can make the organisation more adaptive productive and resilient going forward.
- Protect the organisation's financial viability and reputation by ensuring compliance with financial laws and regulations, rules, standards and policies. This includes both internal and external requirements.
    - This includes understanding the regulatory requirements associated with financial information PCI DSS, SOX.
    - Support the business security team to ensure systems which are impacted by these requirements are protected.
- Protect sensitive, strategic, financial, legal and all risk information.
    - Share only necessary information.
    - Ensure the information is destroyed in compliance with the organisation's data retention policy.
    - Use encryption, passwords and other methods to secure files in transfer.
- Protect access to information repositories.
    - Apply recommended best practice.
    - Implement strong past phrases.
    - Use unique past phrases for each crucial and critical account.
    - Always deploy multifactor authentication.

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.

- Do not share business information on personal accounts.

HUMAN RESOURCES.

WHAT HUMAN RESOURCES DOES.

Planning, hiring and supporting the development, retention and compensation of the organisations workforce.

If you are in the organisation and you are responsible for the management and optimisation of human resources from entry-level staff members to senior executives including external stakeholders this area applies to you.

You direct human resource strategy in alignment with the organisation strategy.

Your role includes human resources, policies and management it also includes talent acquisition and development, workforce and secession planning, culture and diversity, performance management and compensation including benefits.

You matter to the organisation because without your expertise and effort to acquire cultivate and retain organisation's most valuable assets the organisation would not possess the knowledge skills and abilities necessary to succeed.

THE ROLE OF HUMAN RESOURCES IN BUSINESS SECURITY IS ALL ABOUT.

1. Implementing best practice to manage change, train employees and manage performance to enable a cyber secure culture.
2. Ensuring critical cyber security roles are filled consistent with the NICE training framework.
3. Safeguarding sensitive employee information.
4. Implement strategies and tactics to mitigate the risk of insider threat.

WHAT HUMAN RESOURCES PROFESSIONALS SHOULD DO.

- Leverage with the NICE training framework to ensure the proper business security roles are met.
  - Reference this framework for workforce planning, competency deployment and development, talent acquisition and retention.
  - Reference the framework to identify non-cyber security roles which can perform cyber security functions.
  - Apply a standard language to internal conversations to ensure a common understanding across business functions.
- Ensure cyber security knowledge, skills and abilities are incorporated into employee training.
- Mitigate risks introduced by new hires by performing background checks.
- Require and track participation in cyber security training and awareness programs.
- Leverage human resource best practice to retain critical cyber security roles.
- The vigilant to ensure selection of benders that can be effectively maintain the confidentiality of employees personal information.
- Protect access to your human resource management platform by applying best practices such as.
  - Strong past phrases.
  - Unique past phrases for each critical account.
  - Multifactor/2 factor authentication.
- 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.

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.

INFORMATION TECHNOLOGY.

WHAT INFORMATION TECHNOLOGY DOES.

If you define, develop, test, deploy, support, maintain and all protect the business using technological systems this section applies to you.

You are responsible for the function and capability of the business, managing the computer systems and networks that enable quick decision-making and communication and then translate relating that content into processes that run the business.

> *Leveraging technological solutions for business connectivity, productivity, resilience and essential processes.*

You are involved in interaction with end-users so that they can deliver and gather information to their business requirements you work closely with every other organisation component of the business.

Your role in the organisation allows everybody to communicate the systems to capture data, to process that information as required and to manage the systems that all work within the environment depends on.

Critical assets including confidentiality of information, intellectual property, trade secrets, competitive differentiators and also includes customer data so that the organisation can properly use it and protected because of your role.

THE ROLE OF INFORMATION TECHNOLOGY IN BUSINESS SECURITY IS ALL ABOUT.

1. Providing technical expertise for the security of information systems and associated technical platforms.
2. Implement and maintain a robust multilayered defence in depth approach to the information security consistent with best practices.
3. Implement the Cyber security essential 8 security best practices
4. Respond to and mitigate security -related incidents.

WHAT INFORMATION TECHNOLOGIES PROFESSIONALS SHOULD DO.

- Provide technical expertise in support of the organisations cyber security program.
- Provide technical expertise and support of the organisation's IT program.
  - Ensure current knowledge in business security tools, techniques and procedures including secure application and platform design.
  - Cross train other IT roles with security functions provide broader awareness and greater capability within the organisation.
  - Implement best practices where possible.
  - Collaborate with other business function areas across the organisation.
- Implement a robust cyber security program with the appropriate technology and process control in accordance with the organisation's risk mitigation strategy.
  - Leveraged cyber security best practice frameworks.
  - Create standard configurations for all technical requirements.
  - Implement required physical interest controls as needed.
  - Work with external entities including consultants, auditors, professional associations, service providers and required vendor's.
- Integrate business security into IT design, architecture, deployment and routine the management.
  - Consider security at the beginning of all projects not as an afterthought.
  - Integrate security throughout the application development, testing, staging and deployment processes including at the DevOp's level.
- Establish and help to enforce robust security plot policies, processes, procedures and plans for employees, contractors and vendor's.

    - Work closely with senior management to secure support for policies, procedures and processes.
    - Apply the principles of less privilege for access to files and folders.
    - Apply the principles of separation of duties for critical infrastructure, security -related tasks and systems.
- ➢ Implement the essential 8 security best practices
    - Implement and enforce operating system Updates and patching
    - Implement and enforce application updates and patching
    - Utilise multi factor authentication where possible
    - Utilise and implement whitelisting of applications
    - Implement standard operating environment to harden systems
    - Reduce the number of administrators and administrator access
    - Control and manage scripting capability at operating system and application level
    - Implement the 3,2,1 Backup plan
- ➢ Establish, verify and enforce cloud security policies for the organisation.
    - Ensure that cloud services deliver the level of security that the organisation requires.
    - Understand the share responsibilities associated with the consumption of cloud services.
    - Establish and force internal security policies for the use of cloud services.
    - Establish policies and requirements around live data in testing environments.
- ➢ 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.
- ➢ Maintain a high degree of technical competency in knowledge, skills and abilities essential to cyber security.
    - Actively participate in professional associations, conferences and events.
    - Pursue formal education in required relevant fields.
    - Achieve technical certification in cyber security domains as required.
    - Continue to hone skills and demonstrate mastery through participation in car cyber security competitions.

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.
        - o 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.