Introduction

This Guide is intended for executives and managers in both public and private organizations. It is designed to demystify cyber security and to provide a clear, concise and achievable approach to improve any organization's cyber security posture.

Cyber security can seem overwhelming to many. When you hear statistics that thousands of new types of malicious software* are reported each year, it is not hard to imagine the impact a virus or computer compromise can have on our networks and the information contained within those systems. However, if you do not have the knowledge or resources to address these threats, you may feel helpless. Especially for those with a lack of experience or resources to address the constantly evolving and increasing threats from cyberspace, it is difficult to know what to do or how to get started. Often it is the start that stops most of us.

As leaders of your organization, you are responsible for protecting the information in your care. Cyber security is a business function, and technology is a tool that can be used to more securely protect information assets. While addressing cyber security may seem like a daunting task, it is much more palatable if taken in manageable chunks. Cyber security runs the gamut from simple physical security steps (making sure your laptops and other portable media are secured when not in use) to implementing large-scale information technology systems (firewalls, intrusion detection and prevention systems, antivirus and anti-spyware software).

Solutions can be low cost and simple to implement, high cost and complex, or somewhere in between. The important point is to identify what you are responsible for protecting and implement a mix of solutions that best meets your business needs. The good news is there are many resources available to help you establish an efficient, effective and sustainable cyber security program.

This Guide can help provide a valuable first step.

This guide is not intended to be an all inclusive and comprehensive approach to cyber security. It is a first and a very important step in the right direction. It provides real actionable steps your organization can take to enhance cyber security. Let's get started.

Cyber Security Objectives

The objectives below provide a starting point for addressing cyber security needs and developing internal procedures.

A cyber security program should:

- promote and increase the awareness and training of cyber security
- communicate the responsibilities for the organization and individual users' protection of information
- identify threats, vulnerabilities and consequences and take appropriate action
- prepare for the inevitable – disaster recovery, including protecting the availability and recoverability of the organization's information services and missions

Why is Cyber Security Important?

Some examples of how your computer system could be affected by a cyber security incident — whether because of improper cyber security controls, manmade or natural disasters, or malicious users wreaking havoc — include the following:

- Your websites could be compromised and/or unavailable to your users.
- The office computers that your employees use could be shut down by malicious software.
- Someone could break into one of your databases and steal the identity of your employees and customers.
- A disgruntled employee could manipulate or destroy important organizational data.
- A malicious user could use your systems to attack other systems.

These and other cyber security incidents could certainly have a negative impact on your organization.

An unprotected computer is one that does not:

- have antivirus or spyware protection software installed and updated regularly
- have installed hardware or sofware firewall to manage communications between and among networks
- require the user to authenticate (using a password or a token) when logging on
- have operating system and software patches installed and regularly updated

The average unprotected computer connected to the Internet can be compromised in less than a minute. An infected or compromised computer connected to other unprotected computers can easily and quickly pass along that infection, or function as a “backdoor” to your network.

Even a computer without an Internet connection can be cause for cyber security concern. An unprotected machine may not prevent unauthorized individuals from accessing information contained within it. It may become infected through an infected device or media (CD, flash/USB drive or DVD) brought in from elsewhere. Information stored on the computer may be permanently lost due to accidental or intentional alteration or deletion. These are just a few examples of threats to information kept on any computer.

Cyber security incidents can cripple computers and cause a loss of public confidence. Inadequate cyber security measures can lead to the compromise of sensitive information. An oganization has a responsibility to its customers and business partners, both public and private, to safeguard the information with which it is entrusted.