



**SECURIS**

## **Information Security Checklist**

## Copyright

Copyright 1999-2008 © Securis Inc.

## Trademarks

Product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

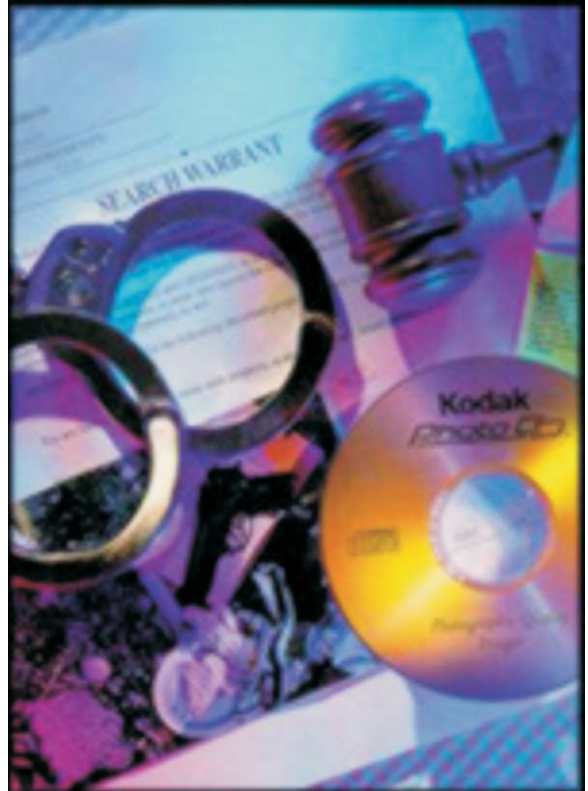


# Introduction

In the span of a few short years, the importance of IT security has risen dramatically as a priority for Canadian businesses. **Cyber threats are real, and can cause serious damage to even the most heavily protected information systems.**

Electronic attacks on corporate and government systems have become commonplace, and stories about hackers wreaking havoc on Web sites and database systems occur all too often. The impact these attacks can have on a company range anywhere from disruption of service and productivity losses to direct financial impact.

In 2001, over 25,000 cyber attacks were detected on Canadian businesses and governments by CanCERT, Canada's first national Computer Emergency Response Team. This number is over 50 times higher than previous tabulations from the year 2000. *And it's only going to get worse.*



An annual survey released by The Computer Security Institute asked respondents from large corporations which information security technologies they implemented at their companies. Nearly **90% of respondents used firewalls and over half of the respondents used Intrusion Detection Systems (IDS); however, 40% reported a system breach from outside of the network during the year.**

The survey also identifies weaknesses in security technologies such as virus scanners. **90% of respondents used some form of anti-virus software** on their workstations and servers, yet **85% of them were infected and financially impacted** by the recent virus/worm attacks. The bottom line is companies are suffering indirect and direct financial loss and technology alone isn't providing the solution to prevent attacks.

A staggering **74% of companies are reporting that the Internet is frequently the point of attack** chosen by intruders. If your company is connected to the Internet, you are exposed to this risk every minute you remain connected. There is an urgent need for information security solutions that can effectively protect a business against these Internet-based threats. The statistics presented in this article should help to reinforce a principle concept of information security: **Hardware and software alone are not the solution.**

**How can you lower your risk?** This booklet outlines some simple measures that can be taken to improve your company's security posture.





# Infrastructure

## Patch software and servers quickly

Over 90% of attacks are attributed the exploitation of a known and preventable security hole. Operating Systems and software applications are typically not secured by default. This allows attackers an easy point of entry into your network. Inventory the operating systems and software your company uses and track vendor Web sites and mailing lists for updates to their software. Applying patches to your software quickly is one of the top defenses against attackers, but frequency is the key.

- **Look for updates to critical business software and operating systems at least twice a year.**



## Ensure critical systems are routinely backed-up

In the event that your company suffers an attack against or loss of important data, the system backup will be your first step to recovery. Make sure all critical systems are routinely backed-up and backup procedures are regularly tested to ensure that recovery is possible. Backup media should be securely stored at different location to prevent damage from a catastrophic loss.

- **The ability to restore from a backup is often over looked and goes untested. Test your restore procedures a minimum of once a year.**

## Ensure your servers, security devices and applications are being logged

The ability to audit information systems is essential in today's electronic business environment. Logging allows you to verify activity on your systems. Without that ability, there is no fail-safe method of verifying a system has not been attacked. If the system has been attacked, logging enables you to measure the severity of the attack and the level of damage incurred.

- **Log not only failed events, but successful ones as well, both are needed to gain full understanding of an unusual situation.**

## Ensure your networks, hosts and applications are being monitored for abnormal activity

Attacks happen quickly and can be difficult to detect unless systems are properly monitored. Weeks or months could go by before any suspicious activity is detected. By this time, the level of damage may be high and the costs to recover may become a financial barrier for your company.

- **Attacks go undetected because of the lack of monitoring of security tools. In-house and outsourced monitoring solutions are available that give companies the assurance they are protected.**





# Accounts

## Enforce good password use

The password is used as the first and sometimes only line of defense for an information system. Simple passwords, such as words or numbers, leave your systems vulnerable. Strong password use is required to ensure your systems stand a chance against an attack. Create and enforce a policy that requires the use of strong, complex passwords.

- **A strong password should have a minimum of seven characters and the use of numbers, symbols, and upper/lower case letters.**

## Create account standards

Users should be given access privileges which are sufficient to perform their tasks, but do not permit them to exceed their authority. Access permissions should be assigned by the appropriate business owners, not IT staff. By default users should have no access or permissions to any information system. From this base, only the minimum required access should be given.

- **Account standards should include password standards, account naming conventions, default access levels and define appropriate “owners” for account maintenance.**



## Remove old accounts

Delete unused or old accounts such as voicemail, e-mail, and other information system accounts. Only current, authorized employees and contractors should have access to your systems using identifiable accounts. Old accounts provide an easy route into your network for attackers.

- **Deactivate old accounts immediately, and remove them once the required tasks and information have been transferred to an active account.**

## Remove group accounts

If your company allows multiple people to login to a system using a shared username and password, you will not be able to uniquely identify a potential intruder or malicious employee. Instead, create separate accounts for each employee with separate passwords.

- **User Accounts should only be used by a single person to ensure ownership and responsibility can be placed on a single person for actions performed by the user account.**





# Procedures

## Instruct employees about the expectation to protect company information

Employees may understand proper use of security technologies, but expectations around employees requirements to protect company data must be explicitly detailed. Security precautions must be taken by all employees to ensure company data and information systems are properly protected. Employee's should be made aware of the meaning of information security and why it is needed in the business place. Stress the importance of complying with information security policies and applying associated procedures. Outline tasks they can perform on a routine basis to help protect themselves and the company.

- **Have employees read and sign an information security policy on an annual basis.**

## Ensure employees are properly trained on how to use security technology

If employees are not properly trained on how security technologies such as passwords, virus scanners and firewalls, employees may circumvent or disable security controls, exposing the company to potential attackers. Training should cover proper use, as well as how to ensure security technologies are working properly.

- **Training around proper use of passwords, virus scanners and other security technology should be done on a regular basis.**

## Establish a personnel dismissal procedure

Create a procedure with human resources to ensure system administrators are notified when employees leave the company. IT staff need to be informed of employee dismissals in a timely and appropriate manner to ensure information systems are protected.

- **Remove all former employee access and control as well as identify and redistribute company data to appropriate resources.**

## Create an Incident Handling plan

An incident handling plan is used to quickly contain attacks and other business threats. The plan defines how people should communicate, what responsibilities they have, and how those responsibilities should be performed in the event of an attack or an information system breakdown.

- **Focus your time and resources on identifying, containing and resolving an issue with confidence and integrity with an incident handling plan.**





# Methodology



## Review authentication methods for remote users

Review how external users communicate and connect to company systems. For users connecting across the web, ensure SSL and other appropriate measures are implemented.

- **Use strong authentication methods comprised of at least two of the following: something you know, something you have, and something you are.**

## Review network communication

Perform a security audit. Review what information and services are allowed in and out of your network. Limit network and Internet access to appropriate levels for business use. Identify any unknown or unwanted network use and remove or block access. Ensure firewalls are configured to block all traffic except for applications and services that management has agreed upon.

- **Identify all points of entry into your network, and ensure all access have appropriate business justification and acceptance from management.**

## Classify company data

Data classification should be done to determine the criticality of company information and identify how each piece of information should be handled. Categorize data based on its business impact, sensitivity and its vulnerability to loss or theft. Once data classification is in place, business risk analysis can be performed when examining how information is protected in storage, transmission, and daily use.

- **Classification should encompass all company information: paper based as well as electronic.**

## Undergo a Vulnerability Assessment from a security vendor

Vulnerability assessments allow you to quickly identify and prioritize vulnerabilities on your network, and measure the effectiveness of implemented security measures. Trained professionals can help you create work plans to patch your systems and protect your company.

- **Focus on critical issues in your information technology architecture by having a vulnerability assessment performed.**

