

# TOP SECURITY TIPS FOR ORGANIZATIONS



## Start at the Top

Security should be initiated, supported, and directed from the top. The ED/CEO needs to be ultimately accountable and there must be ownership and budget to get things done in the organization.

## Get a Plan

A security policy helps you proactively manage risks and map security to your organization's objectives. It needs to address confidentiality, integrity, and availability of your organization and resources.

## Understand Your Assets

What are your most important assets? Facilities? Systems? Client data? How valuable is it? Who has access to it? What can they do with it? Regulations? How much risk can you stomach as part of your security policy?

## Take Stock

You're going to need to get a baseline of your computer systems inventory and health so you know what you have and where the holes are. You'll also need to address existing technical problems before proceeding.

## Include Your People

The people on the front lines are the ones who often know what needs protecting. They also know what restrictions they can live with and still do their jobs. Including them throughout the process is critical.

## Get Help

Security is complex, scary, and confusing. If you don't have qualified staff get help with planning. Work with a trusted IT provider. Beware of someone who wants to sell you something before understanding your needs.

## Keep It Simple

Solutions should be simple and modular. If a system is complex and you don't understand it, it is vulnerable.

## People and Processes

You can't totally automate security. The most secure systems are enhanced with well trained, skilled people.

## Beware the Weakest Link

A system is only as strong as its weakest link. If you protect your important electronic data but don't properly shred and dispose of critical documents you may have a problem. Do you have a policy for data on laptops?

## Implement in Steps

You can't do it all at once and to try and do so could be disastrous. Decide what is most important and create a timeline to phase in your plan and security program.

## Educate & Train

More than half of all security breaches originate from people within organizations—intentionally and unintentionally. Security education and training, especially on organizational policies, should occur at every level.

## Backup Data & Systems

Too many organizations do not have good strategies for data and system backup. Perform regular backups and verification of critical data and evaluate having fallback systems for critical processes (i.e.. Servers).

## Stay Current

Stay up-to-date with the latest service packs for operating systems, Internet applications, virus patches, etc. Newer is almost always more secure. For Windows desktops run XP SP2. No more Windows 9x.

## Stick With It

Security is an ongoing process of managing change, assessment, and improvement. Done right it can reduce catastrophic failures, reduce support cost and time, and increase your ability to plan and manage your IT system. Security is something we must embrace as part of our new digital world!

[www.GaiaICT.com](http://www.GaiaICT.com)  
Phone: 206.369.8840  
Fax: 206.418.0922



INFORMATION & COMMUNICATION TECHNOLOGIES

Copyright © 2006 Gaia ICT

3530 NE 182nd Street  
Lake Forest Park, WA  
USA  
98155-4222