

**WWW.DAYWATCHER.COM**

# What is Information Security?

---

[www.daywatcher.com](http://www.daywatcher.com)

The Business, Technology, Innovation and Digital Media Blog.



# What is Information Security?

---

## **The Reality of Information Security**

Information Security (IS) is often confused with the phrases "computer security" and "Internet security." The term "Information Security" is more encompassing than its computer and Internet comrades, as Information Security includes the protection of the confidentiality, integrity and availability (CIA) of ALL of your information and data (in any form of data, such as electronic, print, etc.), versus just online activities or the security of a computer system. Within the realm of IS, the protection of the CIA Triad comes from ensuring there is no unauthorised access, use, disclosure, disruption, modification or destruction of any form of your data or information.

According to a recent Pricewaterhouse Coopers "Trends in Proprietary Information Loss Survey Report," businesses - regardless of size within the range of small to large - experienced intellectual and proprietary information losses of around £35 billion pounds in the US alone. Almost half of those losses (49%) were within the realm of the companies' R&D, 36% was loss of Customer Lists and associated data, and 27% was Financial Data. These losses are experienced in all countries with parallel magnitude. Such breaches of security can irreparably damage any company, causing lost revenue, legal issues, and even bankruptcy. Finance isn't the only realm of importance, as IS also includes ethical and legal concerns - as evidenced in the 36% loss of customer information.

## **Information Security Hype**

As a career path, the field of Information Security is quickly growing and evolving. But throughout an organisation, Information Security is not the sole responsibility of just one Information Security Officer (ISO). It is the responsibility of all employees and consultants from reception to C-Level. An organisation cannot just hire an Information Security Officer and expect all of the risks to be secured through the efforts of that one party and enacted technologies and procedures. Everyone within the company must buy in, perhaps under the guidance and expertise of an ISO - who in turn follows the strategic direction laid out by his or her CIO. There is no quick fix for IS.

## **Myths of IS**

1. Information Security within organisations is far advanced from one year ago, and we will inevitably advance beyond the potential risks.

Just as security technologies and options are advancing every day, the means of breaching those advanced barriers are also improving and ever-changing. Much as with Newton's Law of Motion ("For every action there is an equal and opposite reaction"), for every security advancement, there is an equal and opposite breach advancement. Information Security is not a means to an end. There will always be threats and risks that must be proactively worked against and overcome.

# What is Information Security?

---

## 2. Technology equals security.

The belief that technological advancements hold the key to IS is false on many levels. Don't forget that Information Security is relative to any form of data and information, not just computer systems, networks and data centres. A simple sheet of paper left on a photocopier or use of public computers for data retrieval while on business travel can be major threats.

## 3. Frequent changes of employee passwords and complex access codes protect data.

While a simple solution at the surface, frequent changes of passwords introduce potential for breaches due to the human element. If you are frequently requiring password changes, users are more likely to record their passwords on pieces of paper within their desks, in wallets, or in spreadsheets, for example. It doesn't matter how complex a password is, if it is so complex that the user has to write it down to remember how to log onto their own system.

## 4. IS staff should consist of only consultants (as they are most qualified) and operate as an individual business unit.

The optimum manner of implementing and ensuring IS is to utilise current staff whenever possible (according to their talents and expertise), and containing IS personnel within each department. There is often that claim that Marketing and Finance departments rarely see eye to eye. The same applies to IS personnel. If they are to communicate throughout the organisation to ensure potential risks are contained, shouldn't the IS personnel speak the language of each of the departments and have intimate knowledge of the delineation of duties (and thus the risks) within those departments? Recruit from within and create a fully infiltrating network of departmental IS experts from your pre-existing human assets.

## 5. Government regulations are the "expert" source for how you should lead your company through IS.

Regulations in IS do serve a solid purpose and work at the best ability of the government to oversee the security of the collective of organisations within a country. However, your company is the expert of where your own risks lie. Don't wait for the government to find the holes in your system, as by then it will be too late.

# What is Information Security?

---

6. The "Human Factor" will always be the biggest point of risk.

It is not necessarily true that its people are an organisation's biggest vulnerability. If a companywide system of expectations, policies, procedures, and accountability is enforced, the corporate culture can move closer toward minimising the risk derived from human error and accidental conveyance of confidential data and information.

In summary, a system of checks and balances, including reward and punishment will create an environment of greater accountability and heightened awareness of the need for company-wide cooperation at all levels.

## **About the DAYWATCHER.COM blog**

The [daywatcher.com](http://daywatcher.com) blog by [Imran Zaman](#) aims to make available free unique articles covering Business, Technology, Innovation and Digital Media.