

## Adoption of information Security standards.

for standard which was preceded by two widely used successful global management system standards, ISO 9001 and ISO 14001, the worldwide adoption of ISO/IEC 27001 is surprisingly low. Two years after its publication, the number of ISO/IEC 27001 certifications is well under that of its two predecessors ISO 9001, quality management, and ISO 14001, environmental management system standards, during the same period. What explains so low adoption, given the importance of information security management as compared to that of quality and environmental issues.

Aiming at obtaining insights on the unexpectedly low and surprisingly uneven diffusion of the ISO/IEC 27001 standard, in the following section we examine successively the drivers for adoption of information security management

Standards, the success factors and the specific cases of employees' adoption. Finally, we explore the barriers and the limitations affecting the adoption of ISMS, and solutions and recommendations to foster this adoption.

### Drivers & barriers for adoption, and limitations of Information Security

One of the major objectives of information security standards is to provide consistent national and international practice: this is the environmental

concern and healthy lifestyle are the main drivers to the adoption. "difficulty in finding" is the greatest barrier to the adoption. Drivers associated barrier to the hedonistic needs tend to positively motivate the adoption. Personal factors (such as age) tend to positively motivate the adoption. Situational factors, as availability and little motivation, can serve as inhibitors.

→ It's a market research type of study that allows companies to study everything they will encounter when expanding.

into a new category to avoid unpleasant surprises.

### Limitations of Information Security

- Provides security to all your information
- Enhances defence against cyber-attacks
- Reduces security-related costs
- Improves company work culture
- Safeguard Confidentiality, Integrity and availability of data.
- As technology increases so will the crimes associated with it. Making the use of information security very worth while.
- It keeps vital private information out of the wrong hands.
- Information security protects users valuable information both while in use and while it is being stored.
- Technology is always changing so users must always purchase upgraded information security.

- Since technology is always changing nothing will ever be completely secure.
- It can be extremely complicated and users might not totally understand what they are dealing with.
- It can slow down productivity if a user is constantly having to enter passwords.
- If a user misses on single area that should be protected the whole system could be compromised.
- Recognising that you are a target.
- Failure to inform employees of threats
- Ransomware attacks
- Missing security patches
- Bring your own device (BYOD) Threats
- Losing sight of the 'backup plan'
- Lack of a corporate security program
- Treating cyber security like an IT issue instead of a financial issue.

## Human factors in security

Human factors are used by cybercriminals to effect unauthorised access, steal and credentials, and infect IT systems and endpoints with malware such as ransomware. Without the human-in-the-machine effect, cybercrime would be much more difficult.

The human factor in cyber security risk is usually termed 'insider threat'. The 'Insider' takes the form of employees and non-employees, such as consultants. The simple fact that insiders are an integrated part of an organisation's processes and utilise IT resources with permission, makes it difficult to address the human failures that lead to cyber security risk.

Insider-related cyber security risk is a major problem: a 2020 Insider Threat report by Cyber Security Insiders points out that 68% of organisations feel "moderately to extremely Vulnerable" to insider threats.

This is not surprising when you look at some of the breaking news cyber attack headlines of the last year, such as the Twitter hack of 2020, where high-profile Twitter accounts, including Barack Obama's, were accessed.

The Human factors that lead to human failures

According to research from IBM, the top three areas to focus attention on when creating security strategies to mitigate cyber security risks are:

1. Phishing
2. Scan and exploit
3. Unauthorized use of Credential

All three vectors have an element that involves a human factor at some point in the attack chain.

### Phishing and spear-phishing - human factors:

This requires a human target to click on a link or open an infected attachment to begin the infection chain.

Often, phishing will be used to target privileged users to harvest their credentials.

Privileged users have access to more important resources - the theft of privileged credentials is their golden chalice of hacking.

Scan and Exploit - human failure!

Hackers use anything that makes life easy and being able to automatically

Scan for vulnerabilities is a useful factor to malware infection. IT system components,

such as web servers, databases and cloud apps, can end up misconfigured if the impact of poor security is not fully understood.

In secure apps and web components results in security holes that hackers can exploit. In this case, human failure leads to cyber security risk.

Unauthorised use of credentials - human failure and human factors. Credential theft leads to unauthorised access to IT systems and resources.

ways that credentials can be used without authorisation include:

\* Shoulder surfing :- Credentials are stolen when a malicious person watches someone enter a password.

Phishing:- tricking a person into entering login credentials into a spoof login page.

Social engineering:- tricking a person into handing over a login credential over the phone, social media, or using other communication methods, such as emails, help desks and texts;

In all three of the most successful hacking vectors, both the human factor and human failure loom large. Cyber security risk is concentrated in our employees and non-employees, but how can we reduce this risk?

## Mitigating the Human Factor in Cyber Security Risk

Make Security a culture - It may sound cliché, but if the notion of security is embedded into your corporate culture, it is less likely that staff will be overwhelmed and afraid when something happens. A culture of security is created using security awareness training to help form positive security habits in employees.

Make it easy to report a security incident - Incidents need to be reported, so that they can be acted upon by the right skilled personnel that reflects the level of risk.

A reporting system, designed to make reporting super easy for employees, will take the pain out of incident reporting and make it more likely to happen.

## Adoption of Information Security standards

The first attempts to publicize information security standards took place in the 1980's, with the publishing of what was called orange and white books by TSEC in the U.S and ITSEC in Europe, respectively.

The evolution of information security standards through the four waves resulted in over a dozen standards with varying degrees of "representation" of each of the waves. Having analyzed five ISMS Overview studies as the departure point, we conducted a further literature search for the standards that were referred to by at least three of the five sources. We found that some standards offer only technical measures, while others provide comprehensive governance frameworks.

## The specific case of ISO/IEC 27000 set of standards

Given the global nature of contemporary business operation and the existence of more than 200 different information security has been recognized by the international business community.

- ISO/IEC 27001 and 27002 Standards are commonly seen as a response to this need, as they represent the building blocks of the ISO/IEC 27000 integrated and global standard.
- ISO/IEC 27001 can be viewed as an overall program that combines risk management, security management, governance and compliance. It helps an organisation ensure that the right people, processes and technologies are in place that are appropriate to the business model.

## Role of information professional :-

- Information professional or information specialist is someone who collects, records, organises, stores, processes, retrieves, and disseminates printed or digital information.
- The service delivered to the client is known as an information service.
- To provide intellectual access to information in any format.
- To evaluate available source of information.
- To organize & structure information to ensure the preservation of information.
- Oversee the library to ensure cleanliness, order and protection of the library resources.

Develop and organize library inventory  
e.g books, collections, periodicals, multi-media

- conduct regular checks and updates on database information.
- The core functions professional include collecting and disseminating printed or digital information.
- The digit someone who deals with handling.
- Information specialist manage the data for their employees and clients and distribute information.
- With the company, we can do all the works of organizations

- The information profession or information specialist is someone who collects, records, organises, stores, preserves, delivers and disseminates printed or digital information.
- In their professional lives, librarians and information professionals work to:
  - Create readers advisory resources to encourage young students to develop a lifelong love of reading.
  - Come compensated anchors the professional and

- The code of ethics for librarians and other professionals defines basic principles binding for all representatives of the profession and identifying their social mission and ethical responsibility in all environments.
- Social mission and ethical responsibility in all environments of their professional activity.
- Working knowledge of relevant operating systems.
- Keen attention to detail.
- Good organization, time management and prioritization.
- Efficient troubleshooting abilities.

#### Qualities :-

Virtually every organization needs an IT technician to support and maintain its computer.

- Attention to detection all the technologies.