INFORMATION SECURITY IN THE WORLD OF CORPORATIONS

BY DIANA GRANGER

Introduction

Information security, or InfoSec, is the practice of defending information from unauthorized access, use, disclosure, or destruction. In its applications to technology, most often some sort of computer system, it is referred to as IT Security or computer security. IT security specialists can be found in almost all major corporations, due to the nature and sensitivity of the data they possess. They protect information from malicious cyber attacks.

IT Risk

Any risk associated to IT can be referred to as IT risk. Factors considered when measuring risk are the value of the assets, the likelihood of the threat, the nature of the vulnerability, and the likely impact the threat will have.

Assessing Risk

The Open Web Application Security Project (OWASP)), is an open-source web application security project whose community includes corporation, educational organizations, and individuals from a variety of places around the world. For measuring risk, the OWASP proposes the following guideline:

- Estimation of Likelihood as a mean of the following factors in a 0 to 9 scale:
  - Threat agent factors
    - Skill level, Motive, Opportunity, and Size
  - Vulnerability factors
    - Ease of discovery, Ease of exploit, Awareness, and Intrusion detection
- Estimation of Impact as a mean of the following factors on a 0 to 9 scale:
  - Technical Impact
    - Loss of confidentiality, Loss of integrity, Loss of availability, Loss of accountability
  - Business Impact Factors
    - Financial damage, Reputation damage, Non-compliance, Privacy-violation
- Rate likelihood and impact in a low, medium, high scale, where 0 to 2 is low, 3 to 5 is medium, and 6 to 9 is high.

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Access Control

Access control as it relates to InfoSec is the selective restriction of access to a place or resource. In computer access control, there are four essential services the system provides:

- Authorization – specification of what the user can do
- Identification – assurance that only legitimate subjects can log on to a system
- Access approval – granting access during operations by association of users with the resources they are allowed to access
- Accountability – identification of what changes the user made

Network Security

Network security consists of the provisions and policies adopted by a network administrator to prenent and monitor a breach in access control, misuse, modification, or denial of a computer network and related resources. The following measures are are typically taken in large business:

- A strong firewall and proxy, or network Guard, to keep unwanted users out
- A strong antivirus software and Internet Security Software package
- Strong passwords which are changed on a weekly to bi-weekly basis for authentication
- Exercising physical security precautions amongst employees
- Network analyzer or network monitor