

# Information Security Management

## Introduction

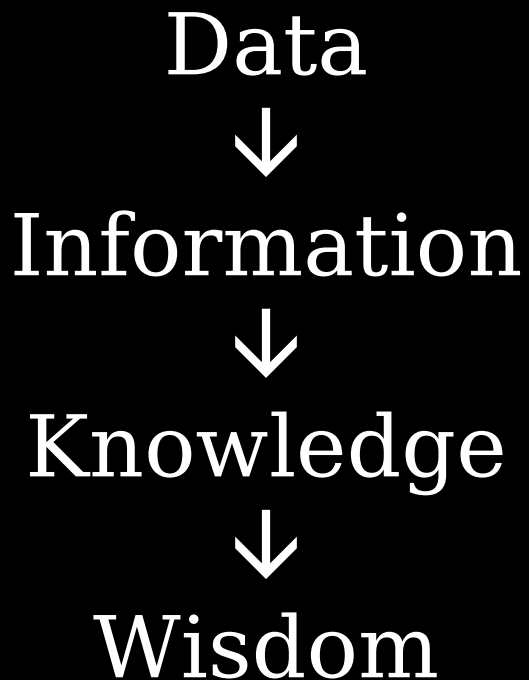
Webster University  
Scott Granneman

What is “information”?

Wikipedia on “information”:

“Information is a term with many meanings depending on context, but is as a rule closely related to such concepts as meaning, knowledge, instruction, communication, representation, and mental stimulus.”

DIKW Hierarchy,  
1<sup>st</sup> developed by Russell Ackoff:



The DIKW Hierarchy helps define the jobs of security pros.

Gathering **data**

(logfiles, visual inspections, asking questions, reading listservs & RSS feeds)



Turning that data into **information**  
(figuring out what is happening to whom,  
& where and when it's happening)



Applying information to create **knowledge**  
("How is this happening?")



Synthesizing knowledge into **wisdom**  
("What can we do to make sure we're safer?  
What are best practices?")

What is “security”?

Bruce Schneier's *Beyond Fear*:

“Security is about  
preventing adverse consequences  
from the intentional and unwarranted  
actions  
of others.”

Wikipedia on “Security”:

“Security is being free from danger.”

Wikipedia on “Security (computers)”:

“Computer security is  
the effort to create a secure computing platform,  
designed so that agents  
(users or programs)  
can only perform actions that have been allowed.”



Security is both a feeling & reality,  
both subjective & objective.

Our textbook's definition:

“The quality or state of being secure—  
to be free from danger”

Security is achieved using several  
strategies simultaneously.

## Specialized areas of security:

Physical security

Personal security

Operations security

Communications security

Network security

Information security (InfoSec)

Computer security

Normally, InfoSec is seen as including:

- Physical security
- Personal security
- Operations security
- Communications security
  - ✓ Network security
- ✓ Information security (InfoSec)
  - ✓ Computer security

What is “management”?

Management:  
A process of achieving objectives  
using a given set of resources.

To manage  
the information security process,  
first understand  
core principles of management.

A manager is:  
“someone who works  
with and through other people  
by coordinating their work activities  
in order to accomplish organizational  
goals”

Managers have several roles.

Informational role:

Collecting, processing, & using information to achieve the objective.

Interpersonal role:

Interacting with superiors, subordinates, outside stakeholders, & others.

Decisional role:

Selecting from alternative approaches & resolving conflicts, dilemmas, or challenges.

What are the differences between  
leadership & management?



A leader influences employees so that they are willing to accomplish objectives.

A leader is expected to lead by example & demonstrate personal traits that instill a desire in others to follow.

Leadership provides purpose, direction, & motivation to those who follow.

---

A manager administers the resources of the organization.

# Characteristics of a leader include:

Bearing

Integrity

Courage

Judgment

Decisiveness

Justice

Dependability

Knowledge

Endurance

Loyalty

Enthusiasm

Tact

Initiative

Unselfishness

# How can you improve your leadership capabilities?

1. Know yourself & seek self-improvement
2. Be technically & tactically proficient
3. Seek responsibility  
& take responsibility for your actions
4. Make sound & timely decisions
5. Set the example
6. Know your subordinates  
& look out for their well-being

7. Keep your subordinates informed

8. Develop a sense of responsibility in your subordinates

9. Ensure the task is understood, supervised, & accomplished

10. Build the team

11. Employ your team in accordance with its capabilities

Yoda has some good advice here.

“No, try not! Do or do not, there is no try.”

“Hmm. Control, control. You must learn control.”

“Fear is the path to the dark side.  
Fear leads to anger. Anger leads to hate.  
Hate leads to suffering.”

“Remember, a Jedi’s strength flows from the Force.  
But beware. Anger, fear, aggression.  
The dark side are they.  
Once you start down the dark path,  
forever will it dominate your destiny.”

A leader must ...

**BE**

a person of strong & honorable character

**KNOW**

you, the details of your situation,  
the standards to which you work,  
human nature, & your team

**DO**

by providing  
purpose, direction, & motivation  
to your team

Three basic behavioral types of leaders:

Autocratic

Democratic

Laissez-faire

2 well-known management approaches:

Traditional management theory  
using principles of  
planning, organizing, staffing, directing,  
& controlling (POSDC)

Popular management theory  
using principles of management into  
planning, organizing, leading, &  
controlling (POLC)



Let's listen to an expert on security.

“Tom Parenty’s mission is to create a common language with which techies and managers can discuss the security of business activities.

He has been a computer scientist with the U.S. National Security Agency, and since the mid-1980s held security-related positions in the software industry before going independent four years ago. He has also testified before a number of U.S. House of Representatives and Senate Committees, and has a new book just out entitled *Digital Defense, What You Should Know About Protecting Your Company’s Assets. ...*

Tom sees two trends that demand this collaboration: that organizations are sharing more information, and that they're doing so without the traditional human intermediaries that act as filters. Traditional security, he says, is designed to 'protect the good folks inside from the bad folks outside.' But the 'line between insider and outsider is becoming increasingly blurred.'"

Tom Parenty,  
interviewed by Doug Kaye  
for IT Conversations  
8 October 2003

<http://www.itconversations.com/shows/detail52.html>

Thanks!