CASE FOR REQUIRING INFORMATION TECHNOLOGIES STRATEGIC PLANS

By B.J. Moore, Lida Ray Technologies

ABSTRACT

Due to the ubiquitous nature of information technologies (IT), our heavy reliance upon them, trust in their output and the sunk cost invested in them, creation and maintenance of solid strategies to safeguard these systems is no longer a luxury. An understanding of the key elements of IT, its data and the potential threats to it are required to develop and manage a solid information technology strategy (ITS). Although some commonalities exist, each instance of an application varies in its criticality, thrust and potential threats. Cost factors and the ever-evolving nature of technology make it impractical to totally safeguard any system. Thus, a desirable ITS achieves a balance which provides sufficient system safeguarding within cost, labor, and other constraints.

INTRODUCTION

Information technologies (IT) and the data they provide are increasingly pervasive throughout all aspects of military and commercial operations. These technologies may be in the form of new tools, add-ons to existing tools or they may be intrinsically embedded in tools. The umbrella of information technologies covers diverse strata of applications. These applications are as varied as intelligence data capture and transmission to logistics planning, information warfare to daily business functions such as payroll, and battlefield operations to avionics. With our increasing reliance on and general trust in information technologies it becomes ever more important to develop thorough strategies for ensuring their security, productivity, accuracy, supportability and currency.

ITS Goals	**Threats**				**System Factors**	
	Inherent	Maintenance	Economic	Human Threats	Complexity	Criticality
Security						
Productivity						
Accuracy						
Supportability						
Currency						

Table 1. Primary Influencing Factors vs. ITS Goals

A solidly designed information technology strategy (ITS) is required whether hostile threats are anticipated or not. Increasingly, daily operations can grind to a halt or become blind with the loss of an IT system. Impacts range from economic loss to loss of life when critical systems in logistics, transportation, health, finance or other fields fail unexpectantly. Often more critical is the harm sustained by functional but damaged systems -- systems that appear to be operating normally but which produce invalid results. This situation may go undiagnosed while our inherent trust in the results creates faulty decisions by system users.

THREATS

Many threats exist to information technologies and to their data. These can be summarized as:

Inherent (design and logic flaws)
Maintenance (calibration, interface, supportability, and obsolescence errors)
Human Threats
Economic (tampering for profit or to create economic gain or loss)
Hostile (both military and civilian hostile action for tactical advantage)
Challenge (where thrill or challenge is the driving motivation rather than gain or destruction)

Inherent Errors

Traditionally, inherent errors such as faulty logic or design errors are expected to be caught and corrected in the design phase. However, for systems of a critical nature or systems being used in a novel way, periodic validation checks may prove invaluable. A well-documented design flaw affecting many computer systems today is the year 2000 date problem. Affected systems utilize a space saving two-digit date field for calculations. Thus, even though operating correctly in every function, they will fail or compute incorrectly when they come across the year 2000 in their calculations.

Maintainability Issues

Maintenance issues includes a broad spectrum of errors or problems which occur generally without specific intent but which can devastate a system's usefulness. Common problems include calibration errors, interface and inter-operability problems, supportability issues, obsolescence and reliability. Calibration errors are self-explanatory. The remaining issues deal with the nature life cycle of products. Overtime, changes in related technology to which a system must interface or interact may render a once working interface inactive. Likewise, as vendors develop newer products, their support for functional but outdated equipment dwindles. Parts, supplies and knowledgeable support personnel gradually diminish in availability while increasing in cost. These changes in a system's maintainability often have little relation to whether the system still operates correctly. A word processor may still compose letters but have no drivers available for current printers, thus rendering it functional but obsolete. Diminishing manufacturing sources for component or even end item parts can also be an issue - especially in non-mainstream systems.

Technical expertise migrates towards emerging technology. For example, COBOL programmers once were the industry mainstay but now are relatively few in number, as COBOL has lost out in the development realm to fourth generation languages. Even though millions of lines of COBOL remain in constant use, the bulk of COBOL programmers have shifted to newer technologies. With the acknowledgment of the year 2000 date problem, demand for COBOL programmers is temporarily high again but costs are even higher due to the scarcity.

An ITS which reviewed maintainability issues periodically would alert the decision maker to diminishing sources, increasing costs and other factors which would indicate when replacement or upgrade should be planned.

Reliability of a system addresses the stability of the system's functionality (commonly called 'Up Time'). Established technology that is unreliable is quickly replaced in the marketplace by more reliable competitive alternatives. Specialty, emerging or under development technology often are the main sources of reliability problems. The cutting edge nature of work being performed on specialty or emerging technology often balances the disadvantages of poor up time and makes the system users more tolerant of reliability problems. Scientists working on research are more willing to put up with frequent system downtime in an experimental or leading edge system yet to be perfected. However, similar bursts of unproductive time would be unacceptable in a system required to perform continuous operation, at needed during critical operations, or merely in mundane day-to-day operations.

Human Threats

Threats perpetrated by individuals with specific intent whether for profit (Economic threats), for tactical advantage (military and civilian Hostile threats) or for the thrill or challenge (Challenge threats) require system and data security plans. If system access is full and open or the data is widely available, many security issues are avoided. However, this is rarely the case. Common security considerations (Shown in table 2.) include safeguarding access and preventing interception, maintaining the system environment, preventing or providing for system disruption, preventing/identifying unauthorized modification, and maintaining the secrecy around closely held technology specifics.

In all cases, when analyzing a potential threat, motives and opportunity should be taken into account. Unfortunately, the very nature of the Information Technologies lends itself to distancing the potential criminal from the crime, thus decreasing a major social barrier to refraining from this type of activity. Setting aside for the moment, the organized Information Warfare Combatant, generally, information related crimes to date have been perpetrated by individuals or small groups. People, both internal and external to the organization can and historically have been the source of IT compromise.

A person who might never be physically violent may easily justify actions that wreck electronic damage, mischief or even ultimately result in injury to people. These people perceive information crimes as victimless in the case of financial crime or crime against faceless entities such as corporations or even individuals they know only as an account name or number.

More deliberate criminal intent is also encouraged by the feeling of being removed from the crime scene and thus removed from the danger of apprehension. This assumption may or may not be true in any situation, but people still harbor the feeling of immunity. Studies repeatedly show personality and behavioral differences in how people react when face to face vs. how they interact on-line. On-line, people demonstrate increased self-confidence and in many cases, aggressive behavior.

There is also the problem of motive. In information technology crimes the motiveless or “thrill” motive comes into play more often than in many other areas of industry. The challenge of breaking a code, penetrating a firewall, inserting a destructive virus, or tampering so skillfully with a code that users are temporarily unaware the data output is compromised unfortunately has a strong appeal to some. The level of knowledge and talent required to perpetrate these crimes runs the gamut from your average kid to the media hyped (but infrequent) “hacker genius” level. Low-level skills and knowledge are sufficient in most cases. The distancing effect of the technology again encourages a sense of invulnerability.

Some thrill seekers enjoy the media coverage of the damage they have created as much or more than the challenge of the act itself. In the case of viruses, creation is only the beginning. Due to the nature of IT and how we use it, the spread of a virus can be rapid, comprehensive and devastating long after it has left the designer’s control.

In the case of the organized Information Warfare Combatant, the motives are broader, less personal. Targets are selected on a strategic or tactical basis. More sophisticated activities may be funded, equipped and undertaken, and finally, larger groups of personnel involved.

ITS GOALS

A workable ITS will seek to achieve a balance of system/data productivity, accuracy, supportability, currency and security specific to the IT instance being safeguarded While these are not mutually exclusive, extremes in any one area will impact the others. The mix of potential threats and system criticality and complexity increase the difficulty of achieving this balance.

Productivity

Productivity Issues are closely related to the maintainability and system accuracy. Productivity factors concern whether the system or data provides the functionality required, is useful, and creates timely output.

Productivity issues:

Usefulness
Timeliness
Functionality

Accuracy

Ensuring accuracy of data / technology is of obvious importance. Since output from Information Technologies is generally assumed valid and accurate, two areas require consideration in an ITS strategy. First, consider the potential security threat of unauthorized modification of the hardware, software or the actual data. In some applications, such as Automatic Landing Systems (ALS), reliance upon data which has been tampered with, even slightly, could result in over or undershooting the landing for a plane. Software tampering such as diverting the third digit of financial transactions into a specific account amounts to fraud but does not pose a safety issue. Second, is the unintended system or data inaccuracy created by miscalibration of hardware, faulty software logic, or data errors imposed through electronically dirty transmission, juxtaposition, or simply poor data entry techniques.

Each type of inaccuracy is important to guard against. The unintended system inaccuracy typically can best be caught and / or prevented in the system design and test phases. The other causes of inaccuracy can occur throughout the system or data life cycle.

Supportability

Topics discussed in the Inherent, Maintenance, and Human Threats area give a broad overview of support issues. Equipment, supplies and technical knowledge abundance and availability are inversely proportionate to the cost of obtaining them. Thus, product/technology life cycle, market trends, and market dominance need to be considered in decisions regarding use, support and timing of replacements for IT. These decisions may be independent of whether the existing system is still functioning properly.

Currency

Currency is sometimes considered a subset of Supportability since it deals with the frequency of updates required, the nearness of the technology to state-of-the-art levels, and the associated maintainability issues.

Security

Security covers many aspects from environment to tampering to maintaining a close hold on technology details. Many traditional system support plans address components of security, thus, a review of those documents is a good starting point for a security review. Analyzing how open the system access and data should be is a fundamental key to determine the security measures required in each area specified. Only a few systems will contain technology that must be extremely closely held for competitive or tactical advantage. Typically, it is the output of the system that contains the material to be safeguarded. Even if the data is considered non-public, the effort invested in its protection should be weighed against other Open Sources Intelligence sources. If the data can easily be obtained, extrapolated, or otherwise compiled from public sources, much less value is incurred by stringent safeguards in this area.

Security covers broad group of issues. These include:				
	• Access / Interception			
		•	Physical	
			•	Access to equipment
			•	Access to data via unprotected terminal, disk, or hard copy
		•	Electronic taps / interception	
			•	Internal
			•	External
	• Environmental			
		•	Physical Environment	
		•	Natural Environment	
	• Disruption			
		•	Temporary	
		•	Permanent	
	• Unauthorized Modification			
		•	Data Input or Output Tampering	
		•	Software Modification	
		•	Hardware Modification	
	• Closely-held Technology Compromise			
		•	Opponent acquires same technology	
		•	Opponent acquires competitive technology	
		•	New technology obsoletes existing	

Table 2. Security Issues

Access issues follow similar considerations. Full electronic access is rarely granted even on public systems, while levels of privilege established within the system is common. These levels can be broad brush by category of user or specific to each individual. System operation and maintenance costs increase as access segmentation increases. The segmentation should reflect the problems arising from too extensive privileges and the potential for harm.

Physical access applies to equipment or to data. Physical data access can be achieved via unprotected terminals, disks, or hard copy. Physical access decisions, like electronic access, should be based upon the potential for harm. For example, an end users' PC would generally require minimal physical security while the network server would be more closely safeguarded. Even physical theft of the end user unit (assuming data backup and protection) would impact only one person while theft of the server would impact most or all users.

Interception of data via electronic methods can be internal or external. Internal interception can be as simple as cable vampire taps or sophisticated as subroutines to split or duplicate transmissions. External forces can use similar methods. Sometimes, the media carrying data is left unsecured with emphasis on securing the actual data itself. Satellite and wireless network transmissions are a good example. The signals are freely interceptable but the data is encrypted to prevent unauthorized use. Prevention methodologies depend on the criticality of the system/data and the physical properties of system components such as in the case of wireless communication media.

Environmental controls should cover the physical and natural environment. System downtime and data loss are equally problematic whether caused by environmental issues such as loss of power, air conditioning failure, fire, or flood or by human threats or equipment failure. Again traditional system specification documents may provide existing information regarding the environmental impacts judged critical to a system and the current measures taken to prevent or recover from a failure.

Disruption, whether temporary or permanent can be caused by numerous factors. These include equipment failure, human error, environmental problems, system overloads (throughput bottlenecks), or deliberate human intervention. Alternate or redundant systems, communication paths or data sources are one option when managing potential disruption. Security and maintainability issues also play a key role in preventing the majority of disruptions. Mission critical systems may need protection from jamming and other electronic warfare techniques.   Analysis indicates economic systems are increasingly being considered as potential targets for electronic warfare.

Unauthorized Modification is more insidious than many of the security breeches discussed so far. This type of tampering relies upon our general trust in the output of systems. Inaccuracy can be introduced unintentionally through design flaws, poor data entry techniques, transposition, corrupt data from other systems, logic faults, hardware miscalibration, or data errors imposed during transmission. Intentional modification can occur at any point in the processing from altering raw data to the final output. Changes to the hardware or software itself are another variation.

Common modifications:

Unintentional modifications
Data Input or Output Tampering
Software Modification
Hardware Modification

IT STRATEGY FORMATION

The diversity of information technology applications requires not one but many strategies based upon the unique needs of the application. Economic, time and manpower constraints preclude any all-encompassing protection / currency strategies. Fortunately, such an extensive protection effort is rarely necessary.

Several factors should be considered when determining how to frame an Information Strategy (IS).   These include:

Nature of application and is criticality
Nature of technology
Whether it is the information or the technology that needs protected
Whether redundant or alternative sources are available
The impact of disruption to technology or information loss
Time required to recover
The importance of supremacy in the technology or information
Potential threats.
Acceptable trade-offs

These factors cannot be isolated from each other when defining the strategic elements to employ. For example, a system that displays raw data such as wind speed requires minimal safeguards when part of a stationary measurement tool on a tower. When the same data is being captured and displayed in a cockpit, its importance takes on an entirely different quality. Thus, in critical applications even raw data may require stringent safeguards to ensure data accuracy, availability, and

Not all information or technology is equal. Some systems contain useful data such as plans data contained on a command and control system, or a series of facts such as failure rates of weapon components in a reliability database or raw data such as intelligence sensor telemetry. Each of these examples requires different safeguards.

Nature of Application

Applications which are add-ons for ease of use in performing some other operation require less stringent protection ITS than applications where the information technologies are an inherent feature. The first case represents *convenience* applications. If a convenience application is disrupted, unavailable, or overcome by newer technology the impact is typically measured more in terms of extra time and effort required to perform the tasks in some manual or other manner.

Embedded information technologies are a different matter. Disruption of an avionics system in flight could have disastrous consequences. Here, disruption or unavailability could be measured in lives lost.

Nature of Technology

Technology employed today varies from the most unsophisticated, outdated systems to the most cutting edge, sophisticated ones. Each has its place and each requires differences in management. The nature of the technology is a defining factor in selecting the level of system currency required.

Outdated technology does not imply a lack of functionality; merely that newer options exist. Even so, many uses do not fully exploit the functionality available from the outdated technology. An outdated word processing system used primarily to generate simple letters is impacted by its lack of currency only when a) additional features are needed which it doesn't offer or b) systems which it interacts with move beyond it to the point at which the interface is difficult or impossible to maintain. For example, a word processor attached to a dot matrix printer and which interacts with a spreadsheet may have no currency requirements until the printer is replaced with a laser printer for which no driver exists in the word processor or until graphical interpretations from the spreadsheet need to be imported and this feature is not supported by the word processor.

Even in the event that currency becomes an issue, the level of currency required still requires consideration. For mundane applications, upgrading each time a new feature or version comes out is not necessary. Periodic upgrades to the current standard are acceptable to maintain ease of operation, ease of interaction with other systems, and broad common functionality in many cases.

Technology used for applications such as battle space dominance requires the other extreme in currency maintenance.   In this type of application, technical equality or superiority over enemies, can determine the outcome of a conflict. Information technologies that provide information on enemy and ally troop locations and disposition provide valuable situational awareness of a theater of operation. Maintaining state-of-the-art technology can mean having equal or greater visibility in the theater than the opponent.

Increasing Application Criticality	
Mundane	Critical
Periodic upgrades acceptable	State-of-the-art technology may be required

Table 3. Technology Currency vs. Application Criticality

Nature of Data

As collected raw data is sorted, organized, and analyzed into information and finally coalesced into knowledge; its criticality increases geometrically.   Raw data, such as gathered from stand-off sensors, whether used for intelligence or satellite tracking, requires more emphasis on ensuring redundant or alternative sources while security becomes increasingly important as data is transformed into information then to knowledge. Limiting access also becomes significantly more important as data moves towards knowledge.

Raw Data	Information	Knowledge
Emphasis on....		
Timeliness Accuracy Redundant sources.	Accuracy Access Security	Security Limited Access

Table 4. Raw Data Through Knowledge   Areas of Emphasis

Summary

Requiring creation and maintenance of solid Information Technology Strategies (ITS) to safeguard our systems/data is no longer a luxury. Due to the ubiquitous nature of information technologies (IT), our heavy reliance upon them, trust in their output and the sunk cost invested in them, failure to safeguard these systems/data can result in economic, military, or human vulnerability.   Thorough understanding of the key elements of IT, its data and the potential threats to it are required to develop and manage a viable ITS. Common IT factors to be considered include:

System / application / data criticality

Budget for ITS aspects (including costs of not protecting the system)
System / application / data redundancy or alternate sources
Labor and time constraints
Overall system cost
Level of system complexity
Level and types of safeguards required (includes access, environmental, disruption, etc.)

Although some commonalities exist, each instance of an application varies in its criticality, thrust and potential threats rendering a broad brush ITS practically useless. At the same time, cost factors and the ever-evolving nature of technology make it impractical to totally safeguard any system. Thus, a desirable ITS must achieve a balance which provides sufficient system safeguarding within cost, labor, and other constraints.

Author Biography

B. J. Moore, President of Lida Ray Technologies, provides strategic planning services and risk management to DoD contractors and Fortune 100 multi-national corporations. She has authored over 100 technical papers and journal articles and has been a guest speaker at international conferences. She is listed in Who's Who in Science and Engineering and Who's Who in the World. Ms. Moore holds degrees in Electronic Engineering, Computer Science, and Business Administration. Her major interest areas are in emerging technology insertion, strategic planning, and wireless systems.