Information Security: The Human Perspective

Kathleen M. Carley

August 2000

Direct all correspondence to:
Prof. Kathleen M. Carley
Dept. of Social and Decision Sciences
Carnegie Mellon University
Pittsburgh, PA 15143
Email: kathleen.carley@cmu.edu
Fax: 1-412-268-6938
Tel: 1-412-268-3225
URL: http://hss.cmu.edu/departments/sds/faculty/carley.html

This work was supported in part by the Office of Naval Research (ONR), United States Navy Grant No. N00014-97-1-0037, NSF IRI9633 662, NSF IGERT: CASOS, the Pennsylvania Infrastructure Technology Alliance, a partnership of Carnegie Mellon, Lehigh University, and the Commonwealth of Pennsylvania's Department of Economic and Community Development. Additional support was provided by ICES (the Institute for Complex Engineered Systems), CASOS – the center for Computational Analysis of Social and Organizational Systems at Carnegie Mellon University (*http://www.casos.ece.cmu.edu*), and the Heinz School of Public Policy and Management at Carnegie Mellon University. The views and conclusions contained in this document are those of the author and should not be interpreted as representing the official policies, either expressed or implied, of the Office of Naval Research, the National Science Foundation or the U.S. government.

Information Security: The Human Perspective

Kathleen M. Carley

Abstract

For many organizations, information security threats are within the organization. Core intellectual property, key knowledge, and information on core processes reside in the minds of employees and can be transferred to other companies as employees take new employment opportunities. Disgruntled employees can turn on the company and modify key processes, destroy information, or leave taking critical intellectual property with them. This paper discusses a combined social network and knowledge management approach to discovering organizational vulnerabilities within companies.

Information Security: The Human Perspective

One of the major security problems in organizations today is that personnel give their passwords away.   Organizations are more likely to be attacked by their own employees than by outsiders. Core intellectual property, key knowledge, and information on core processes reside in the minds of employees and can be transferred to other companies as employees take new employment opportunities. Such knowledge is rarely captured in an adequate fashion in databases, human resource records, and organizational accounting information. Recent cases of industrial espionage all point to human errors in gathering or searching for information, corrupt or disgruntled employees, and miscommunication or misunderstandings. Information security is a system level problem and can only be adequately addressed if both technological and organizational issues are considered simultaneously.

How should organizations be designed to reduce their vulnerability to information errors from a human perspective? As part of the new program in information security at the Heinz School, a new course - "Organizational Management and Information Security" - begins to address this question. In this course, organizational issues related to information security are addressed from a human centered perspective. Issues of security at the individual, organizational and inter-organizational level will be discussed. Topics covered include critical employees, redundancy, cascade effects, organizational memory, organizational learning, information diffusion, changing belief structures, personnel vulnerability analysis, knowledge management, and information warfare.

The Meta-Network Perspective

The structure of organizations, the incentives individuals face within organizations, the social networks they build, the training they receive, and the degree of autonomy and authority all influence the level of security risks faced by an organization. Moreover, organizational structures which inhibit exposure to information security risks are often at odds with structures for facilitating group level innovation, minimizing redundancy, maintaining individual privacy, enabling flexibility, and promoting adaptiveness. This course examines the issue of how to design an organization for security, how to locate security risks in an existing design, and what other aspects of individual and organizational performance may be affected by creating an informationally secure organization.

Organizational structure is characterized in terms of the networks of relations that link people, knowledge and tasks as well as the procedure and institutional arrangements for changing the number of these entities (e.g., hiring and firing procedures, training procedures, etc.).   These networks form a meta-network. In Table 1 the meta-matrix representation of this meta-network is shown for the three components that are key to security – personnel, knowledge and tasks. This representation of the meta-network is an extension of the original PCANS formulation to knowledge (Krackhardt and Carley; 1998; Carley and Krackhardt, 1999). Using this representation we can classify existing social network, operations research, and information processing measures of organizations (Carley, Ren and Krackhardt, 2000). This particular representation also underlies many existing models of organizational design, performance and adaptability such as VDT, ORGAHEAD and ORGMEM. Analysis of organization's ability to learn, based on an understanding of this scheme, suggest that although the networks in the meta-network co-evolve, the relative rate of evolution affects the underlying culture of the organization and its decision making processes (Carley and Hill, 2001). In Table 1, the network in each segment of the meta-network is shown in italics. Then, in each cell illustrative measures are listed of security risks that can be measures using data in that particular cell.

Table 1. Meta-matrix Representation of the Meta-network Useful for Addressing Information Security Within Organizations

	Personnel	Knowledge	Tasks
Personnel	*Communication Network* *Who talks to whom* Isolates Critical Employee	*Knowledge Network* *Who knows what* Inevitable disclosure Critical Employee	*Assignment Network* *Who does what* Assignment Redundancy Critical Employee
Knowledge		*Information Network* *What information is related to what* Missing Information Links	*Needs Network* *What knowledge is needed to do what task* Information Redundancy Identification of Security Critical Points
Tasks			*Precedence Network* *What task must be done before which* Critical Path Tasks

Using this formalism we can mathematically represent the organizational architecture as a set of matrices linking personnel, knowledge, and tasks. We denote the number of personnel as P, the number of pieces of knowledge as K, and the number of tasks as T. In Table 1, we show the following 6 networks: communication network (PxP), knowledge network (PxK), assignment network (PxT),. Information network (KxK), needs network (KxT), and precedence network (TxT),

For each of the network in the meta-network, measures of the organizational architecture exist – such as span of control, complexity, and redundancy. In fact there are a large number of such measures. Most measures are for "square" or mxm matrices such as the communication, information and precedence networks. There are also measures for the "rectangular" or mxn matrices such as the knowledge, assignment, and needs networks. In addition, there are a number of security related measures such as those shown in Table 1.

The overall meta-matrix is a representation of a multi-color network. Personnel, knowledge and tasks are nodes, each of a different color or type. The overall network, as it links nodes of different colors, is thus a multi-color network. This meta-network is nxn and so most standard network measures can be used; however, doing so violates the implicit assumption of uniformity of meaning across relations and unity of type of node. One consequence is that new interpretations of standard measures need to be developed when they are used on multi-color networks. Another implication is that new measures need to be developed that utilize multiple sub-matrices in the over all representation of the organization’s architecture.

Using these networks we can begin to predict changes in communication patterns, vulnerability to turnover, which personnel need to leave before core technological processes are inevitably disclosed to a competitor, path by which rumors are likely to propagate, changes in beliefs, and so forth. Changes in these networks can be examined for changes in the distribution of power and workload which can minimize or increase the degree to which personnel are motivated to work in the corporation's interests. Examining multiple structures at once lets you address complex security issues such as whether the need to communicate in order to coordinate getting a set of coupled tasks finished is leading to sufficient knowledge sharing that the performance of the organization can be disrupted by inhibiting that communication.

Organizational Vulnerability

Comparison of two organizational architectures in the meta-matrix representation enables the researcher to determine the relative efficacy of different types of attacks on the organization’s security. An organization is vulnerable if it is possible, at minimal cost to degrading its performance, the consensus among personnel, or the rate at which information diffuses through the organization. Additionally, it is possible to increase an organization’s vulnerability from an information security perspective; e.g., by increasing the number of critical employees and making inevitable disclosure possible. Performance and vulnerability for an organization should be assessed using numerous measures.

There are many ways to attack an organization from an information security perspective. In the meta-network this is basically done by adding or dropping a node (person, piece of knowledge or task) or by adding or dropping one or more relations (one of the links in one of the networks in the meta-network). Illustrative types of information security attacks:

- Eliminate one or more employees; e.g., by hiring them away.
- Add one or more new employees.; e.g., by hiring new personnel.
- Reassign personnel ; i.e., change who reports to or talks to whom.
- Retask personnel; i.e., change who is doing what.
- Eliminate or stop doing a task.
- Increase the probability of access error.
- Increase the probability of processing error.
- Increase the probability of communication error.

ThreatFinder

ThreatFinder is a software application program developed at Carnegie Mellon for the express purpose of evaluating security threat in organizations given information on the networks in the meta-network. The user enters a meta-matrix representation of the networks for an organization, hypothetical or real. Then a series of threats are evaluated including critical employees and potential loss of information. In addition, the user can use ThreatFinder in a what-if fashion to determine how the performance of the organization is likely to change if various attacks are made such as the hiring away of a critical employee. Table 2 contains illustrative output from ThreatFinder for the event of hiring away 1 critical employee in a hypothetical company.

Table 2. Illustrative ThreatFinder Output

Event – hire away 1 critical employee

Capability	**Before Attack**	**After Attack**
Cost of Communication Channel	100	100
Cost of Re-assigning an Agent	1500	1500
Probability of Access Error	.1	.25
Probability of Processing Error	.1	.2
Probability of Communication Error	.05	.15
Performance	.88	.75

Unfortunately, within both the organization and the social network literature there are few measures that cross the boundaries of personnel, knowledge and tasks and use more than one of the sub-matrices in the overall architecture. Building off of the work of Galbraith, Thompson, and the work in cognitive science, a variety of such measures were constructed and are available within ThreatFinder. An example of such a measure is the need for communication. Another measure is cognitive load. The measures available in ThreatFinder were chosen because a) they are commonly used, b) they enable a logical measurement of the sub-matrices, c) they formalize a common security concern, or d) they use a wider number of sub-matrices or a different combination of sub-matrices. In addition, each of these measures is arguably a predictor of organizational vulnerability, performance or adaptivity.

Using ThreatFinder to analyze a company it can be seen that there is no single right company design. There are many different organizational architectures that make sense from a security perspective. There is also a tradeoff between performance, innovation and vulnerability. Increasing organizational performance can at times increase and at other times decrease the organization’s vulnerability and potential to be innovative.

Educational Application

This approach to information security and the associated ThreatFinder software are taught in the Information Security and Organizational Design course at Carnegie Mellon University. This course takes an interdisciplinary perspective to information security and draws on recent research in information systems, organizational theory, sociology, social psychology, cognitive science and computer science. At the theoretical level, the course is tied together by the concept of networks and knowledge management. Students learn techniques for mapping and analyzing the knowledge network, information network, and the communication network within and among organizations. The capstone of the course is the SECURITY GAME a multi-week project to design and attack a company.

The Security Game

The capstone of the course is a security game in which students work in small teams to design a hypothetical organization that is informationally secure. Students develop a company description subject to financial constraints, cognitive and physical constraints on agent behavior, and task requirements. They try to design companies that maximize expected performance and minimizes information vulnerability. Performance is assessed using a simulation model of team decision making. Vulnerability is assessed using a series of network measures ranging from potential for inevitable disclosure, vulnerability to typical attacks, vulnerability to personnel problems such as rumor propagation and employee dissatisfaction.

Then each student team attacks all other organizations. That is, they are given an attack budget and are told to device a plan of attack subject to financial constraints that will decrease the other organization's performance, internal consensus, and/or make it more vulnerable to future attacks.

References

Carley, Kathleen M. & Vanessa Hill, 2001, "Structural Change and Learning Within Organizations". In Dynamics of Organizations: Computational Modeling and Organizational Theories. Edited by Alessandro Lomi and Erik R. Larsen, MIT Press/AAAI Press/Live Oak, Ch. 2. pp 63-92.

Carley, Kathleen M., Yuqing Ren & David Krackhardt, 2000, "Measuring and Modeling Change in C^3I Architecture." *In Proceedings of the 2000 Command and Control Research and Technology Symposium*, Naval Postgraduate School, Monterey, CA, June 26-28, 2000.

Carley, Kathleen M. & David Krackhardt, 1999, "A Typology for C^2 Measures." *In Proceedings of the 1999 International Symposium on Command and Control Research and Technology*. Newport,RI, June, 1999.

Krackhardt, David & Kathleen M. Carley, 1998, "A PCANS Model of Structure in Organization" Pp. 113-119 in *Proceedings of the 1998 International Symposium on Command and Control Research and Technology*. June. Monterray, CA.