2008

Information Sharing and Emergency Services: An Examination Using Information Security Principles

Wm. Arthur Conklin
University of Houston, wconklin@uh.edu

Information Sharing and Emergency Services: An Examination using Information Security Principles

Wm. Arthur Conklin
College of Technology, University of Houston
waconklin@uh.edu

ABSTRACT

This paper explores issues associated with information sharing with emergency services entities through the lens of information security, structuration theory and agency theory. Information sharing can result in moral hazard that needs to be addressed to facilitate information transfers needed during emergency services. Developing a solution to the moral hazard issue associated with information sharing in emergency service situations is a time sensitive issue that needs to be done prior to the needed sharing of information. This paper illustrates the challenges and opportunities that exist with respect to information sharing between users and providers of emergency services. Based on sound principles of agency theory and structuration theory, a framework to alleviate concerns and maximize information sharing utility is presented. The understanding afforded by the framework will assist both parties to in their efforts to effectively share and yet protect information that is vital to both emergency response and information owners.

Keywords

Information sharing, information security, moral hazard, asymmetric information, agency theory, structuration theory.

INTRODUCTION

Much has been written and discussed about how society has entered the Information Age. Yet for this age to be effective, information must be shared between parties. We share information all the time – when we purchase something with accredit card, we share information, and in return we get a convenient method of conducting transactions. And there are times we choose specifically not to share, but rather protect information from disclosure, as in the case of various corporate financial records, trade secrets and customer information. Information security is a common term for the activities taken to protect information, but it is in reality a much broader field, and includes elements essential to proper information sharing. Proper management of information resources includes the inclusion of a risk based analysis of security needs associated with the information (Conklin et al. 2004). Information sharing has long been a backbone of law enforcement and justice department activities, as information is shared between investigative agencies and later during prosecution (The Global Infrastructure/Standards Working Group 2004). Yet sharing information has been identified as a continual weakness in coordinating national level responses to major emergency situations (Dr. Helen Miller et al. 2005; Kean et al. 2004). The National Commission on Terrorist Attacks on the United States (the 9/11 commission) identified the importance of information sharing (Kean et al. 2004). This paper explores issues associated with information sharing between emergency services personnel and the parties they serve in an emergency. The examination will be through the lens of structuration theory and agency theory, and constrained by information security desires of the party receiving emergency services.

Information systems associated with emergency management have been investigated with respect to form, functionality and design (Chen et al. 2004; Chen et al. 2005; Turoff et al. 2004). The events of 9/11/2001 have fueled a lot of interest in improving information handling associated with emergency services. Secondary uses of information collected by government entities have now become timely. Previous studies have identified that privacy issues can occur with personal information and first responders (Kim et al. 2006). This paper examines theory associated with a party's behavioral decision process associated with sharing of personal information. Emergency services present a unique opportunity for information sharing. One aspect of the information sharing event is the matter of urgency. Another unique aspect is the selection of specific information sharing partners. One side of the information sharing arrangement is the entity of the emergency service provider, typically a local governmental entity. The other side of the information sharing can be a firm, an individual person or some group entity. The concept of information sharing between a government entity and the constituents that it serves is common, but this relationship is usually a well known, documented interaction that is well understood by all parties. What

makes the emergency services relationship unique is the randomness of the event that triggers the sharing event and identifies the affected parties. An examination of the information sharing under these conditions with respect to implications and concerns of all parties is presented. Based on principles of agency theory and structuration theory, a framework to alleviate concerns and maximize information sharing utility is presented. Using this framework, planners can properly prepare to minimize the risk associated with the information sharing, reducing the moral hazard to the contributing party.

EMERGENCY SERVICES

Emergency situations are by definition those where the normal rules of operation are modified, as concern for risks to personnel and property are increased in importance. The systemic response of society in response to emergencies is typically overseen by government entities, local fire departments, emergency medical response units, and for larger events regional, state or federal responses to assist in coping with the issues surrounding the emergency. Emergencies can be the result of numerous causes, the last decade seeing major refinery fires, natural disasters including wild fires and hurricanes, and terrorist incidents, such as the 9-11 attack. Each of these emergency conditions has its specific characteristics and required levels of response from various agencies, but one thing is common across all of them, shared information can lead to better decision making during these critical response times.

There is a wide range of information that can be useful to emergency responders and improve their ability to respond to an incident. In the event of an individual medical emergency, information about the person having the emergency, including medical information, family information, etc. can be useful to responders. If the person having the emergency is unable to provide this information, the firm may act as a third party and share what it knows with regard to these items. In the event of a fire in a chemical plant, accurate inventories, including piping, control systems and associated chemical information can be of use to a responder. In the case of a large natural disaster response, such as the recent southern California wildfires, details of how many personnel, and who they are for remote locations can be valuable information. Also, information regarding remotely controlled infrastructure elements, telecomm, network, SCADA, etc. can be of assistance as emergency responders may need to manipulate these systems in response to environmental systems.

In each of these cases, the information needed by emergency services personnel can also be of value to outside entities, and the firm has a desire to properly secure this information from outside disclosure. In the case of medical records, and family records, the corporate responsibility to protect privacy aspects of this information is codified in a series of laws including HIPAA regulations. In the case of operational details of a firms operation, this information can be of significant use to a competitor, hence firms are reluctant to release this type of information. The issue is not that a firm may feel that the emergency responders are competitors, but rather that once released, they have little or no control over secondary uses.

INFORMATION SECURITY

Information security is a broad field with many aspects. Of importance to information sharing are the concepts of Confidentiality, Integrity and Availability. Confidentiality is the principle of protecting information from disclosure to unauthorized parties. Integrity is the principle of protecting information from unauthorized alteration. Availability is the concept that for authorized users, information will be available when required. Associated with the aspect of these concepts is that of an authorized user, which implies some form of authorization and authentication. Another security concept, non-repudiation, deals with the concept that a party does not have the ability to deny an action that they have taken. For the purposes of this research, non-repudiation, authorization and authentication are considered to be issues that can be stipulated as completed.

To understand the level of required security aspects associated with a specific piece of information is a complex task. The information owner must decide several key elements for the information. First, the importance of the information to the firm is a key driver – if it is a competitive advantage that is also a trade secret, it needs greater protection than an element of information that is publically available. After importance is determined, each of the separate dimensions, confidentiality, integrity and availability need to be considered. Some information requires significant levels of confidentiality, others integrity is more important, and some is driven by availability. Integrity and availability may be more important during medical crises, and confidentiality may be more important with specific elements of personally identifiable information (PII). To insure the appropriate levels of protection occur, the information owner needs to define the levels of these factors required and the conditions associated with them. This determination must be done element by element with respect to a set of information.

AGENCY THEORY

Agency theory is a body of knowledge associated with the understanding of the relationship between a principal and an agent, with the agent acting on behalf of the principle with respect to some form of transaction. Agency theory is concerned with resolving a conflict problem that can occur in agency-principal relationships (Eisenhardt 1989). This conflict problem arises when either the desires or goals of the principal and agent conflict, or when it is difficult or expensive for the principal to verify the actions of the agent. The problem is that the principal cannot verify that the agent has behaved in the desired manner. This problem also arises when the principal and agent have different attitudes toward risk. The problem is manifested because the principal and the agent may prefer different actions based on their different risk preferences. With respect to information sharing, the secondary use of information by an agent, for uses other than that assigned by the principal represent a form of this conflict.

Moral Hazard

Moral hazard is the concept that an entity's behavior will differ based on its understanding of the level of risk to which it is subjected. Moral hazard arises when an entity has some form of shield against risk associated with some activity (Arrow 1963; Holmstrom 1979; Holmstrom 1982). This shield is typically in the form of transference, where the risk is transferred to a third party. In the case of insurance, one party pays another to assume some aspect of risk. Moral Hazard complements the agent problem through the concept of information asymmetry. Information asymmetry arises when two different parties to a transaction have differing levels of information concerning the transaction. It is typically presumed that the Agent will have better information than the principal, and moral hazard postulates that the agent will act based on this information asymmetry. Agents can also have secondary uses of the principal supplied information, which benefit the agent as opposed to the principal. When the agent is shielded from repercussions, either through lack of oversight or lack of control exercised by the principal, then moral hazard situations can occur.

The presence of moral hazard can act as a retarding force, limiting the willingness of a principal to share information with an agent. This is exacerbated in the case of emergency services, where the principal does not actually choose the agent, and is compelled to share information with a party not of its own choosing. Although the principal may have a reasonable reason to share information with the emergency service agent, there is the lingering issue of "how else will this information be used?" that will be considered prior to use. Resolution of the concerns associated with this moral hazard condition needs to be resolved before the need for the transfer occurs to prevent the wasting of valuable time when an incident occurs.

INFORMATION SHARING

Information sharing is the legitimate and purposeful sharing of specific information by design between two parties. Purposeful indicates that both parties have a legitimate reason for the exchange, for the giving party to agree to the sharing, there must be some aspect of exchange in return. This exchange may come in the form of enabling action, where the sharing of information enables the other party to do something. Information sharing can be broken into two main components, on being technical and the other being policy oriented (Relyea et al. 2005). This paper focuses on the policy oriented aspects of information sharing, leaving the technical implementation as future research.

With respect to emergency services, this exchange will typically be of the form with the government emergency service entity acting as an agent on behalf of the party to whom they are responding. The emergency service entity may need incident specific information to better perform their mission and better serve the other party. An example would be a person in a firm that collapses and is unable to respond. On scene EMS personnel would be well served if the firm knew of an existing medical condition, such as diabetes that could lead to such an incident. Disclosure of this information to the on scene personnel by the firm results in a degree of risk. Although the primary reason for the information would be to assist the care of the patient, secondary uses such as disclosure through open records can result in future harm to the patient. This is an example, where a secondary use may be an unintended consequence type action, resulting in harm or risk that is not necessarily anticipated by the principal when the information is requested.

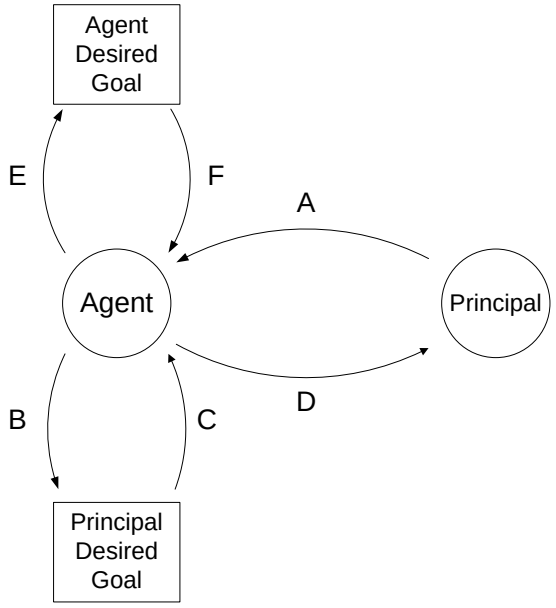

Figure 1. Information Flows in an information sharing event

The notion of exchange between two parties brings up the concept of agents and principals. Using agency theory nomenclature, the party with the information will be referred to as the Principal, and the recipient of the shared information, the Agent. A principal will communicate to the agent information needed for the agent to achieve some goal on behalf of the agent. The information flows, as shown in figure 1, are labeled A, B, C, and D to accomplish this task. A secondary use of the information on the part of the agent is shown as paths E and F, and these represent additional uses of the principal's information for the sole benefit of the agent.

The two paths E and F represent secondary uses of the information being shared that is not to the benefit of the principal and in fact, may be detrimental to the principal. EMS personnel that receive personal identifiable information associated with a specific call, record that information in public records for the purposes of improving the care provided to the patient. Future use of this information, which can be released or sold to third parties, can act as a privacy violation, e.g. the number of lawyer marketing letters received after an accident.

A savvy principal may recognize that there exists a series of both known and unknown risks that accompany some intended benefit, and weighing these risks decide not to share the information. This is a natural reaction to an un-moderated moral hazard problem and illustrates one of the primary impediments to information sharing. Even in cases where the associated risks are not real, but merely imagined, the lack of relief mechanism from the moral hazard issue results in a decision not to share information.

SECONDARY SHARING

A recently confirmed position of the government involves the desire to widely share information (Kean et al. 2004; Relyea et. al. 2005; The Global Infrastructure/Standards Working Group 2004). Of particular note are the following passages:

> Any member of the justice community can access the information they need to do their job, at the time they need it, in a form that is useful, regardless of the location of the data (The Global Infrastructure/Standards Working Group 2004).

and

> Information sharing must occur across agencies that represent divergent disciplines, branches of government, and operating assumptions (The Global Infrastructure/Standards Working Group 2004).

These passages indicate both a desire to engage in information sharing and a desire to use the information shared for additional secondary uses. The very act that created the Department of Homeland Security contains provisions for

information sharing (Section 892, subsections 1-5) and for restrictions of secondary use of federal information (Section 892, subsection 5) (Congress 2002).

IMPLICATIONS

Information sharing can be seen to be a useful activity, yet it is also easy to see the risks. Information that is shared may be subject to secondary, unauthorized uses by the agent. The true nature of these secondary uses may, or may not be understood by the principal, this the creation of the moral hazard associated with sharing. There are several avenues that can be used to address this moral hazard situation. The first of these is the creation of trust between the agent and principal. Trust can be defined as the understanding of how another will act under a given set of circumstances. Trust can be created both by reputation and by track record. People routinely trust websites with their credit card information, expecting the firm to use the number is a specific fashion, and not use it in an unauthorized fashion. To strengthen any element of moral hazard associated with these transactions, a third party element of insurance in the form of liability limits enforced by the credit card issuer. When trust is not an option, or will not apply, other options are needed to manage the moral hazard aspect and to facilitate the information transfer. Regulation is often cited as a means for dealing with broken or dysfunctional markets, and some form of regulation can be applied in the case of information sharing. Regulation is the means that the federal government uses when sharing information with lower level government agencies. The language of the Homeland Security Act specifically mentions that federal data shared with other entities remains the property of the federal agency that shared, and any secondary use is prohibited (Congress 2002).

Regulation may seem to be an easy answer, but it has some inherent complications. The "no-secondary use" clause used by the federal government, if applied to all information sharing, would contradict the government's stated desire to maximize its use of information. If some less restrictive form of limitation were to be mandated, this would require the information provider to provide some form of desired restrictions. This may be done through a documented form of desired levels of confidentiality, integrity and availability for each data element. Additional aspects of limited restrictions would include defining how far a firm can go in its restriction, to prevent complete across the board ban of secondary uses, making the information unavailable for government sponsored secondary use. Remedies in the form of penalties for violation of sharing restrictions would also be needed.

Currently there exist no major control mechanisms over the secondary use of information with the exception of information supplied by the federal government. In the case of emergency services, the agent will typically be some form of governmental entity, e.g. local fire department personnel or other form of first responder. This makes the enforcement of anti-secondary use restrictions more challenging as the majority of principals will not be in a position of power to enforce their desired restrictions over the governmental entity. This only leaves principals the option of limiting information sharing, which is not an optimal solution.

To resolve this issue requires a change in the current information sharing landscape between firms and emergency service providers. The determination and implementation of effective information sharing regulations to remedy the moral hazard solution will require several things to occur. First, both parties will need to address their level of understanding of the sensitivity of specific data elements and levels of reasonable protection. This will take time and effort, and rapidly becomes a non-generalizable solution that has many additional pitfalls (Holmstrom 1982). A method for producing a general solution to the problem can be found in structuration theory. Structuration theory postulates that there is a balancing act between agent action and structure. Structures can be created to enable specific agent actions, and at the same time, specific agent actions can create structures.

The structure associated with emergency services is unique in several ways. First, it involves a time sensitive need to share information, and the need can be critical with respect to reducing the risk associated with further damage or injury. This critical nature of the information sharing need, coupled with the time sensitivity can increase the importance of the sharing need from the perspective of both parties to the event. Although the specifics associated with each event and the required information sharing elements may differ from event to event, there exists a bounded subset of risks that can be mitigated. Each individual person may regard their own PII differently with respect to secondary uses; the range of responses can be bounded and used as a proxy for the collective concern. Ultimately, it could be argued that the agent has less at stake in the engagement, for further damages will typically not be borne by the agent, but instead by the principal. As the agent serves the collective constituency of principals, oversight by governmental bodies will apply pressure to the agent to minimize additional damages and loss. The creation of an environment conducive of information sharing can act as the seed for structuration based changes that will reinforce and maintain a shift in moral hazard equilibrium.

The demand on the part of principals to end secondary uses, even when such secondary uses may benefit the collective of all principals is one of the first steps. A moderation of this demand, based on information risk, sensitivity by type of information to secondary use that effects the principal's defined confidentiality, integrity and availability concerns will act as a second step towards a proper sharing environment. The codification of the agreed upon secondary use limitations will act as an enabler for future information sharing events, leading to a self sustaining environment built upon the interaction of the environment (need for rapid sharing) and actors (the agencies involved in the information transfer). In this form, structuration theory posits that a solution is not only achievable, but if truly mutually beneficial to both parties, that it is sustainable in practice.

CONCLUSIONS

Resolving the problems associated with information sharing will not be an easy task, nor one with a single solution. This paper has examined this problem from the perspective of emergency services constituents sharing information with government agencies. Under most circumstances, this path of information is compelled when the participant is an individual. And the person shares the information because it seems useful at the time, and secondary uses are rarely thought about. But after the fact, the secondary uses can cause loss of trust. Add this experience to issues such as the IRS selling information off tax returns, and other incidents of secondary uses that are felt by some to be privacy violations and the seed is planted. With regular reminders in the news media concerning government uses of information, i.e. DHS data mining, and NSA based phone surveillance, the seed of distrust grows into a major problem. Removing trust from the solution set leaves fewer solutions. Assuming that prohibiting all secondary uses is also off the table, means the solution lies between the extremes.

The time sensitive nature of the required information sharing event means that any negotiation of terms must be done in advance of the needed transfer of information. Complicating the matter is the 1:n nature of the problem. But examining the framework presented and the bounds of the problem and solutions are available. The framework suggests that moral hazard needs to be solved. Structuration suggests that building a self-reinforcing solution will lead to one that spreads throughout the environment. Removing moral hazard requires some means to either restrict the agent's secondary use, or provide some protection for parties sharing information. The challenge becomes one of deciding how to restrict such secondary uses and in what fashion. The security industry concepts of risk, confidentiality, integrity and availability, when applied to specific data elements provides some assistance.

Information shared with governmental agencies in an emergency situation can be used to improve services for a party directly affected by the emergency. Additional use, such as criminal background checks, can also improve services for society. Other uses especially any that lead to data disclosure to entities outside the law enforcement community become more difficult to justify. This will require a change in governmental doctrine on information sharing, albeit a minor one. Law enforcement based reuse still remains a valid strategy. But other forms need to be evaluated. This is one of the areas for future research. Research needs to be conducted on various constituents concerns on the moral hazard problem and their evaluation of risk mitigating strategies. This will lead to an empirical based solution, backed by theory that will assist in making information sharing more of a reality when it counts – when information is needed in an emergency.

REFERENCES

1. Arrow, K. "Uncertainty and the Welfare Economics of Medical Care," *American Economic Review* (53:5) 1963, pp 941-973.
2. Chen, H., Wang, F.Y., and Zeng, D. "Intelligence and security informatics for homeland security: information, communication, and transportation," *Intelligent Transportation Systems, IEEE Transactions on* (5:4) 2004, pp 329-341.
3. Chen, R., Sharman, R., Rao, H.R., and Upadhyaya, S. "Design principles of coordinated multi-incident emergency response systems," *IEEE international conference on intelligence and security informatics*) 2005.
4. Congress, U.S. "Homeland Security Act of 2002," *Public Law*) 2002, pp 107-296.
5. Conklin, A., White, G., Cothren, C., Williams, D., and Davis, R.L. "Principles of Computer Security: Security+" and Beyond,") 2004.
6. Dr. Helen Miller, Joel McNamara, and Dr. Jon Jui "Hurricane Katrina - After Action Report ", OR-2 DMAT (ed.), House Oversight Committee on Government Reform, Washington DC, 2005, p. 16.
7. Eisenhardt, K.M. "Agency Theory: An Assessment and Review," *The Academy of Management Review* (14:1) 1989, pp 57-74.

8. Holmstrom, B. "Moral Hazard and Observability," *The Bell Journal of Economics* (10:1) 1979, pp 74-91.
9. Holmstrom, B. "Moral Hazard in Teams," *The Bell Journal of Economics* (13:2) 1982, pp 324-340.
10. Kean, T.H., and Hamilton, L. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* WW Norton & Company, 2004.
11. Kim, J.K., Sharman, R., Rao, H.R., and Upadhyaya, S. "Framework for Analyzing Critical Incident Management Systems (CIMS)," Proceedings of the 39th Hawaii International Conference on System Sciences, Waikoloa, Hawaii, 2006.
12. Relyea, H.C., and Seifert, J.W. "Information Sharing for Homeland Security: A Brief Overview. Congressional Research Service," *The Library of Congress (Updated January 10, 2005). Available at www. fas. org/sgp/crs/RL32597. pdf*) 2005.
13. The Global Infrastructure/Standards Working Group "A Framework for Justice Information Sharing: Service-Oriented Architecture," GISWG, 2004.
14. Turoff, M., Chumer, M., Van de Walle, B., and Xiang, Y. "The Design of a Dynamic Emergency Response Management Information System (DERMIS); submitted to " *Journal of Information Technology Theory and Application* (5:4) 2004, p 35.