REDUCING THE INFORMATION TECHNOLOGY SECURITY RISK IN MEDICAL SUPPLY CHAINS

Christopher L. Rees, Bioinformatics and Genomics, The George Washington University
crees@gwmail.gwu.edu
Jason K. Deane, Department of Business Information Technology, Virginia Tech
jason.deane@vt.edu

ABSTRACT

With medical information increasingly being shared electronically, the likelihood of increased information security incidents, such as hacking and worm attacks, rises dramatically. It is well-known that managers of organizations do not know either how much money to spend to mitigate information-security attacks, or in what matter to spend it, much less what to do when several organizations are connected in tandem or a so-called supply chain.

This paper utilizes an approach developed previously by one of the authors to minimize risk for a single organization and shows how to extend it to organizations connected in a supply chain. Questions of equity are then addressed such as how the increased cost of risk mitigation should be allocated to members of the chain.

INTRODUCTION

Medical information is increasingly being shared electronically among health care providers, customers, insurance firms, and online health services, and the instances of such sharing seem to be escalating rapidly. For example, Google is now offering personal health records to the public, and more than two dozen institutions have announced that they are partners with Google Health, including CVS, Walgreens, the American Heart Association, Quest Diagnostics, Beth Israel Deaconess Medical Center, and the Cleveland Clinic [8]. In a second (and different) type of example of electronic access, hospitals and individual doctors make their computers accessible to drug companies and other suppliers. In a third paradigm, telemedicine, medical information can be transferred via the Internet or other networks for the purpose of consulting. Such electronic access can be both real time (synchronous) or store-and-forward (asynchronous); real-time telemedicine can be as complex as robotic surgery. Medical specialties deemed conducive to synchronous consultation include psychiatry, family practice, internal medicine, rehabilitation, cardiology, pediatrics, obstetrics, gynecology, neurology, and pharmacy, although not all such applications will always involve computers [11]. (Currently, many involve video conferencing.)

Much technological progress has been made in providing security such as firewalls and antivirus software not just in medicine, but in both the non-medical public and private sectors. Yet in the face of increasing numbers and magnitudes of IT security threats, security managers do not know how best to allocate available funds – or in many cases even the level of the expenditures needed. Furthermore, evidence exists that there is often no correlation between increased spending on such initiatives and actual improvements to the overall security record [1]. In short, although there is no shortage of security standards and research, managers generally have no proven and reliable methodology for measuring the effectiveness of their security initiatives or for assessing the monetary value of their efforts. The

managerial situation is exacerbated when organizations connected in a chain result in additional attacks upon one another, often because a weaker member (security-wise) is connected to the others. Moreover, it is not clear how the significant costs of mitigating IT security costs should be borne by the various members of the chain, particularly when the risk is lower for a weaker member.

This paper first reviews the literature regarding risk mitigation for a single organization. Then work is presented which shows how the single-organization case may be extended to supply chain scenarios. Finally, several supply chain configurations are outlined for which the analysis and results will be provided at the meeting.

MODELING RISK IN A SINGLE FIRM

There is substantial research on the general topic of IT risk, including applications of systems risk [10], economic models [6][7], game theory [2], and value at risk [7]. Rakes, Rees, and Deane [9] have developed a risk-based solution methodology that determines risk for a given set of managerial security choices. Deane, Rees, and Rakes [3] then extended this work by embedding that methodology within a genetic algorithm controller, thereby providing an optimization capability. For a specified budget, with this approach, managers can now make optimal (or near-optimal) security choices to minimize risk to their organization.

The Need for Fuzziness

There is an additional concern making the modeling of risk in an organization difficult – the inability to express threats, countermeasure performance, and asset impacts with precision or crispness. Managers often admit that they have no proven and reliable methodology for measuring the effectiveness of their security initiatives or collecting data needed for making strategic decisions and assessing the monetary value of their efforts. Fittingly, the U.S. Department of Homeland Security recently named a lack of real-world data on risk factors as one of the most pressing information security research problems [12].

The Rakes, Rees, Deane [9] and Deane, Rees, Rakes [3] papers both address this managerial concern of uncertainty. They do this by not merely using expected (unitary) values for threats, asset costs, and countermeasure effectives. Rather they model each of these with fuzzy sets [4][5][13]. They calculate the overall organizational risk as a fuzzy set by using the alpha-cut method of combining fuzzy sets. The genetic algorithm then calculates the centroid of the system risk, and attempts to minimize that value by selecting alternative security controls. The result is the optimal (or near optimal) set of security controls for management to implement, given a specified budget level.

Supply Chain Exacerbation

To date, no work has been done to minimize IT security risk *in a supply chain* either with or without the inclusion of fuzzy risk. The presentation at the SEINFORMS conference will detail how these calculations should be performed for the more general case of threats, asset costs, and countermeasures represented by fuzzy sets.

HIGH-LEVEL ANALYSIS

IT-security, risk models for the different simple supply chains shown in Figure 1 will be built. The chain in Figure 1a is the simplest case where two organizations are connected to each other, one “downstream” and the other “upstream.” A simple example of this might be a single drug supplier connected to a

doctor's office or to a hospital. Figure 2 indicates how the downstream organization can infect the upstream entity. In Figure 1b, three suppliers are connected to one doctor or hospital. In the third case, three organizations are connected in tandem; this case might represent a supplier to a drug company, the drug company itself, and a hospital – all connected in series. Admittedly, these models are simplifications of the connections that do and will occur in practice, but the purpose here is to provide high-level insight and a first step into the basic behavior of IT security in supply chains.

Once these models have been built, the investigation of supply chains can begin. There are a plethora of research issues, ranging from whom to include as chain partners, to how to control the chain to minimize risk, to how one defines equity in the realm of supply-chain security.

Stated differently, this stream of research will be important as it will provide insights, previously unknown, as to how each firm in a chain should act to secure itself from IT threats. It will also furnish results as to how other firms in the chain can be affected by a single organization's behavior, and whether the costs of providing the security to all are proportional to the benefits enjoyed by each.

Findings will be presented in Myrtle Beach at the meeting in October.

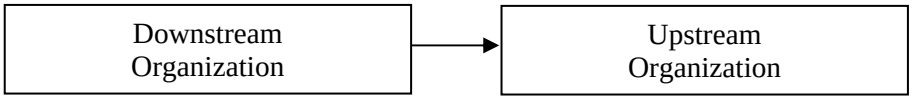

Figure 1a. One downstream organization and one upstream organization.

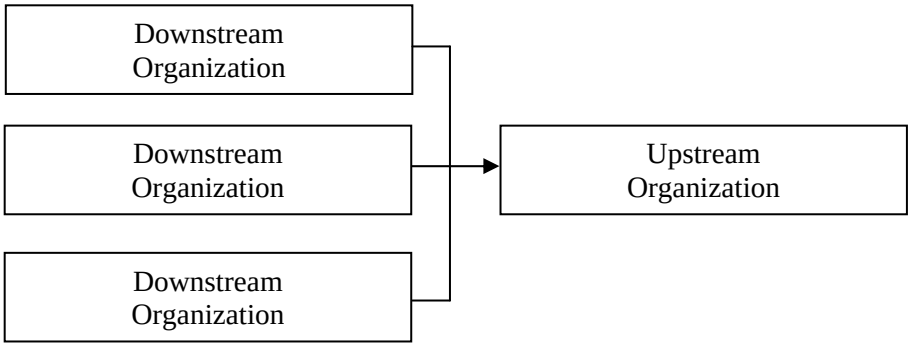

Figure 1b. Three downstream organizations and one upstream organization.

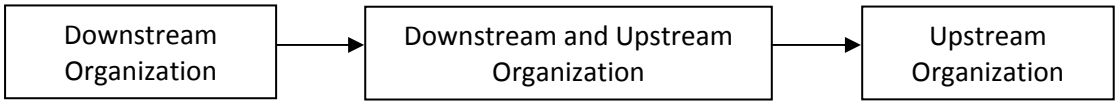

Figure 1c. Three organizations connected in tandem.

Figure 1. Three different configurations of supply chains to be examined.

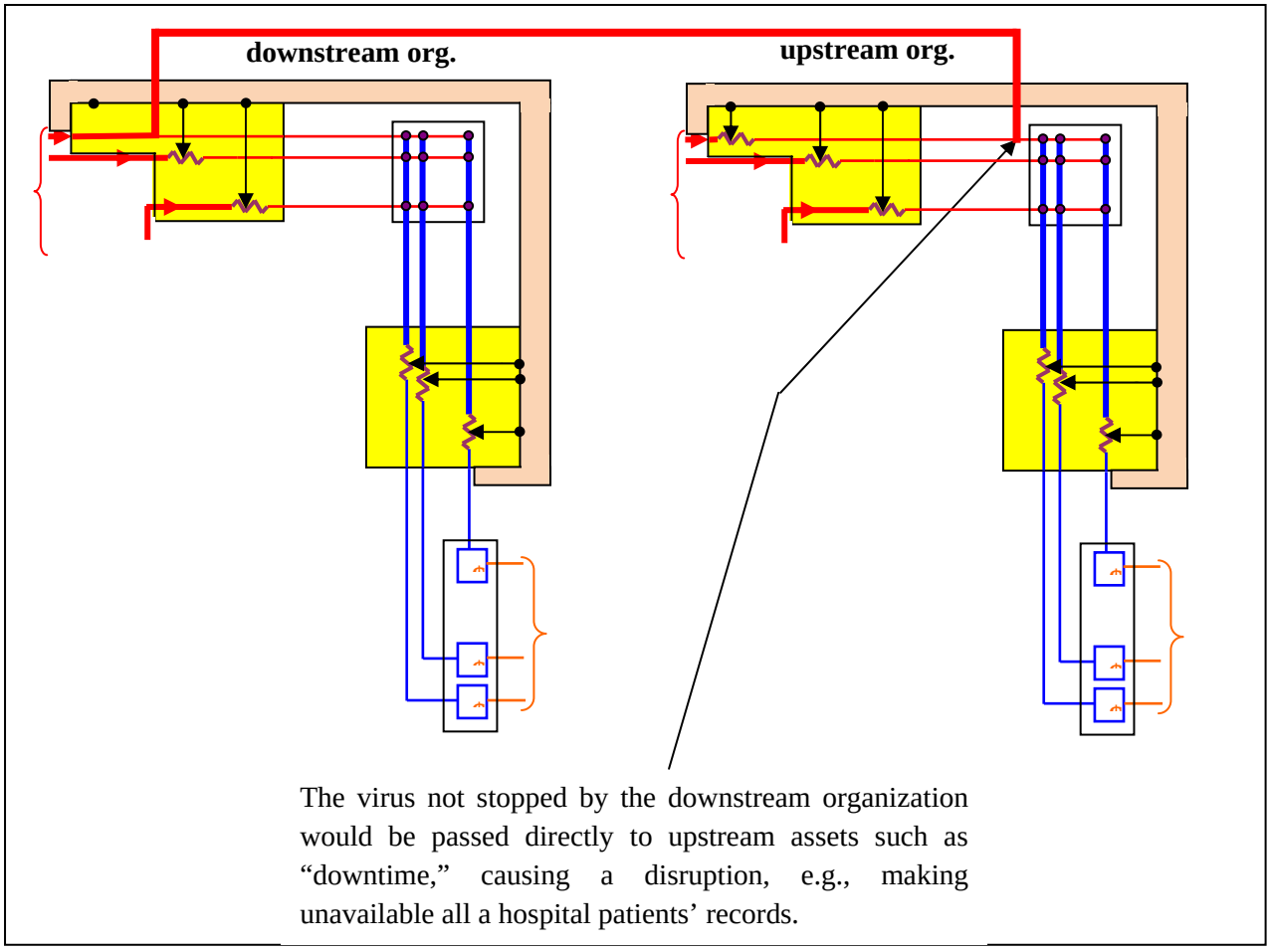

Figure 2. An example of a mechanism whereby one organization passes a virus to a supply-chain partner.

REFERENCES

[1] Berinato, S. "The State of Information Security 2003." *CIO Magazine*, October, 2003.

[2] Cavusoglu, H., Mishra, B., and Raghunathan, S. "A Model for Evaluating IT Security Investments." *Communications of the ACM*, 2004, 47(7), 87-92.

[3] Deane, J.K., Rees, L.P., and Rakes, T.R. "Managing IT Security Using A GA Controller To Direct A Fuzzy DSS." Working paper, 2008.

[4] Dong, W.M. & Wong, F.S. "Fuzzy weighted averages and implementation of the extension principle." *Fuzzy Sets and Systems*, 1987, 21, 183-199.

[5] Fuzzy system. Fuzzy control system, accessed March 28, 2007, available at http://en.wikipedia.org/wiki/Fuzzy_system.

[6] Gordon, L., and Loeb, M. "The Economics of Information Security Investment." *ACM Transactions on Information and Systems Security*, 2002, 5(4), 438 – 457.

[7] Jaisingh, J., and Rees, J. "Value at Risk: A Methodology for Information Security Risk Assessment." In *Proceedings of the INFORMS Conference on Information Systems and Technology*, Miami, Florida, November 2001, 3-4.

[8] Lohr, Steve. "Google offers personal health records on the web." New York Times, May 20, 2008, available at http://www.nytimes.com/2008/05/20/technology/20google.html

[9] Rakes, T.R., Rees, L.P., and Deane, J.K. "Incorporating Uncertainty Into Cybersecurity Risk Planning Using A Fuzzy Support System." Working paper, 2007.

[10] Straub, D.W., and Welke, R.J. "Coping with Systems Risk: Security Planning Models for Management Decision-Making." *MIS Quarterly*, 1998, 22(4), 441 – 470.

[11] Telemedicine. Telemedicine, accessed May 20, 2008, available at: http://en.wikipedia.org/wiki/Telemedicine

[12] Verton, D. "DHS Seeks Real-World Data on Security Breaches." *Computerworld*, September 20, 2004.

[13] Zadeh, L.A. (1965). "Fuzzy sets." *Information and Control*, 8, 338–353.