Cutter Consortium

Executive Summary

Chinese Wall:

An Information Security Approach

by Sebastian Konkol, Senior Consultant, Cutter Consortium

Enterprise Risk Management & Governance
Executive Summary Vol. 8, No. 1

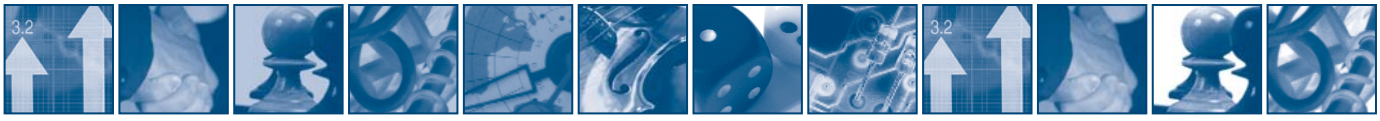
In today's business realities, there are circumstances in which traditionally employed information access schemas are incapable of securing information against breaches. Such a class of problems can be identified as sensitive information security related to conflict of interests. The nature of this conflict is a central issue in today's information security problems and must be addressed in order to protect company assets and reputation.

CONFLICT OF INTERESTS

Businesses today are forced to work in various fields simultaneously. Some companies, such as telecom carriers, trading houses, law firms, professional advisors, must represent many viewpoints concurrently, acting congruently on behalf of their customers' conflicting interests. Such circumstances, when not handled properly, could lead to a situation where one customer's win is the other customer's loss or could even break some legislative regulations. Each circumstance involving an information security breach, particularly for more powerful customers, results in a strong and substantial loss of credibility for the company or even an imbalance of competitiveness in a certain market.

Recently, I have been working on a very specific endeavor: a program involving the largest fixed telephony carrier in Poland (Telekomunikacja Polska [TP]) and a Polish telecom market regulator (Urzad Komunikacji Elektronicznej [UKE]). Historically, there has been a long-lasting dispute between the two parties regarding monopolistic business, which has been practiced by the national carrier. The central issue claims that TP, a provider of broadband Internet access services in both the retail (aka consumer) and wholesale (aka business partner) markets in Poland, discriminates against its wholesale customers (which are TP's competitors in the retail market) in favor of its own retail sales division. Such business practices are quite standard in "balanced" markets, but the telecom market in Poland is not balanced; the biggest company (TP) holds almost 70% of the market and its closest competitor is almost 10 times smaller. In such circumstances, competition does not exist; this is not only bad for small companies but also for consumers. The situation, although smaller in scale, is quite similar to the story of AT&T in the US, before that company was split into several independent, narrowly specialized companies. Some analysts reported that TP's monopolistic attitude was the major obstacle for growth in the number and quality of Internet broadband access services in Poland. This endeavor provides the background for the accompanying *Executive Report*.

The information security issues discussed in the report are not only related to the telecom market; conflicts of interests are quite common in today's business environment and can typically generate negative consequences. Imagine a financial brokerage company that employs traders. Each trader can access the company's customer proprietary information in order to handle transactions appropriately. Consequently, each trader must act on behalf of several brokerage company customers. Everything is fine as long as customer transactions remain independent. However, one trader could serve two transactions that are somehow related to each other, such as selling from one side and buying from the other. The trader, knowing the positions of the two companies, could act favorably toward one of them (rendering the whole transaction as win-lose) or even *optimize* the transaction to maximize its own profits, such as via transaction fees (rendering the transaction results as lose-lose). In either case, the brokerage company loses much more — its credibility in the eyes of customers.



CHINESE WALL SECURITY POLICY

The scientific community dealt with the information security problem in the 1980s. The effort back then resulted in a proposal for an information security system, designed specifically to detect and prevent situations that would lead to conflicts of interests. The system, presented by David Brewer and Michael Nash in 1989, is known as "Chinese Wall security policy" (CWSP).[1] The model received ample critique for its level of complexity and the strong constraints it puts on an organization implementing it. Even so, CWSP has been an inspiration for a whole set of derivative works, which eliminated most of its defects.

Although progress has been made regarding IS capabilities and many things that were beyond the imagination of Brewer and Nash are quite obvious today, some difficulties related to CWSP implementation remain valid. Looking at the overall requirements from a broader perspective, the report examines both security architecture and its implementation.

It is a well-known fact that the weakest link in every security system is the human user. Believing that securing information access on the level of information systems would be sufficient is naive. Many additional organizational measures should be taken to create an environment where CWSP implementation across the scope of an information system can be reinforced. This requires both the user and external party (i.e., partners, outsourcers) to be aware of how business processes run in general as well as to understand the entire security system's continuous improvement mechanisms.

CWSP IMPLEMENTATION

The report illustrates CWSP implementation through the complex IS environments of large companies. It provides some theoretical background; introduces architectural solutions such as IS design, an enterprise architecture viewpoint, and an integration approach; examines organizational measures to be undertaken (for employees and external partners); and suggests an implementation approach (one that is risk-based and agile rather than "big bang"). Each aspect is illustrated with practical considerations, resulting from my experience gained while working on the endeavor described earlier.

Although criticism of the early workings of CWSP as a means of enforcing confidential information access control was quite substantial, there are cases today where traditionally employed information access frameworks would not resolve the issues at stake. IS technology has made so much progress that some of the initial problems related to CWSP implementation are much more easily resolved today. Adding a risk-based approach to the implementation itself makes it possible to rationalize the effort and investments spent on such an implementation, making the whole endeavor agile. In short, Chinese Wall security policy is a vital alternative today as a means of solving difficult information security problems.

ENDNOTE

[1]Brewer, D.F.C., and M.J. Nash. "The Chinese Wall Security Policy." *Proceedings of the IEEE Symposium on Security and Privacy*, IEEE, 1989.

About the Service

Cutter Consortium Enterprise Risk Management & Governance Advisory Service

SENIOR CONSULTANTS

Robert N. Charette, Director; Stephen J. Andriole; Robert D. Austin; Edmund H. Conrow; Sara Cullen; Tom DeMarco; Lynne Ellyn; Andrew Fried; Jerrold Grochow; Scott Hastings; Rebecca Herold; Sebastian Konkol; Steven R. Kursh; Tim Lister; Gerald H. Peterson; Carl Pritchard; Mark Seiden; Mike Sisco; Scott Stribrny; William Zucker

FOR MORE INFORMATION

For more information on Cutter Consortium's Enterprise Risk Management & Governance Advisory Service or its other services, contact: Tel: +1 781 648 8700; Fax: +1 781 648 8707; Email: sales@cutter.com.

 Print ISSN: 1554-7035 (*Executive Report*, *Executive Summary*, and *Executive Update*); online/electronic ISSN: 1554-7043.