Using Information Security as a Response to Competitor Analysis Systems

Lawrence A. Gordon
and Martin P. Loeb

To protect your firm's valuable business data from competitors, sometimes it's best to think like competitors and take a walk in their shoes.

The seminal book by Porter [9] emphasized the need for organizations to perform competitor analysis (CA). The research on CA in the 20 years since the book was published has grown significantly and rapidly (for example, see [1, 12]). One aspect of this literature addresses issues related to developing competitor analysis systems (CAS) [4, 5, 11].

CAS seems to be entering an era of almost unlimited vistas due to the information age. In fact, nearly every organization is both a CAS predator and CAS prey in today's IT environment.

The flip side of studying CA is to study the notion of competitive responses (see [1, 2]). In today's information environment, a logical competitive response to having your firm become a part of the CAS of a rival firm is information security. Of course, firms already expend much effort and funds to protect company information that would give rival firms a competitive advantage. Surprisingly, however, the literature concerned with CAS has not explicitly addressed the issue of information security. At the same time, the information security literature has not explicitly addressed the CAS issue. The purpose of this article is to rectify this situation. More specifically, our first objective is to present a game-theoretic framework that demonstrates how information security is the appropriate rival response to CAS. The primary focus of this framework is using information security to prevent rival firms from including sensitive information on your firm in their CAS. Our second objective is to argue the use of information security as a response to CAS can be logically viewed as a five-step process we call the "CAS defense plan."

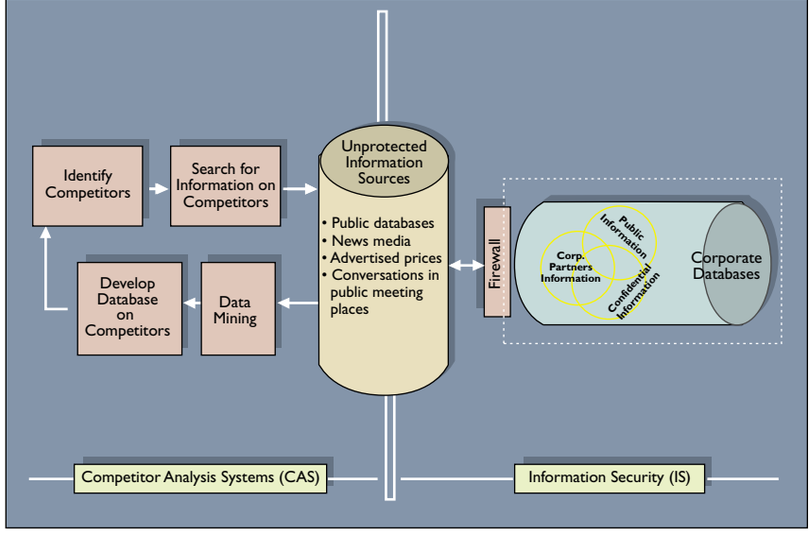
The classical economic markets (that is, pure competition, monopoly, oligopoly, and monopolistic competition) are essentially defined in terms of the type of competition confronting an organization. Furthermore, the parameters defining each of these economic markets place significant constraints on how firms must operate to be successful. However, while providing a useful theoretical frame of reference, most organizations do not operate in a neatly defined economic market. In addition, the market in which a firm operates often changes over time (for example, the market for computer manufacturing firms has changed substantially over the past two decades). As a result, a fundamental activity of modern organizations is the ongoing analysis of the competition. In the strategy literature, CA has taken on a central role in helping organizations get positioned in the marketplace.

There are several dimensions to CA. However, a common theme throughout much of the CA literature is discovering ways to gain a competitive advantage within a defined marketplace (for example, see [9]). Understanding and predicting the behavior of competitors are key aspects of this theme [1]. Predicting competitor responses is also central to this theme [2]. Of course, the process of discovering ways to gain a competitive advantage is based on the notion of gathering information on competitors. In other words, developing some sort of formal CAS is critical for effective analysis [9].

Recent developments related to information technology have moved CAS to center stage. In particular, the role of computers, publicly available databases, the Internet, and data analysis techniques (for example, data mining) now permit a level of CAS unimaginable even a decade ago. As a result, firms have invested in a variety of CAS-related activities. Although the specific type of information gathered will vary from organization to organization, there is little doubt that the development and use of CAS are central activities of most modern organizations (for example, see [5, 6]). Of course, as organizations develop CAS on their rivals (actual and potential), their rivals are doing the same in return. The low cost of computers (hardware and software) and inexpensive access to reams of public databases has virtually assured this prey and predator aspect of CAS.

The more your competitors analyze your firm's activities, the more valuable it becomes for your firm to view information security as a competitive response. In other words, information security can be

Figure 1. Competitor analysis systems vs. information security.



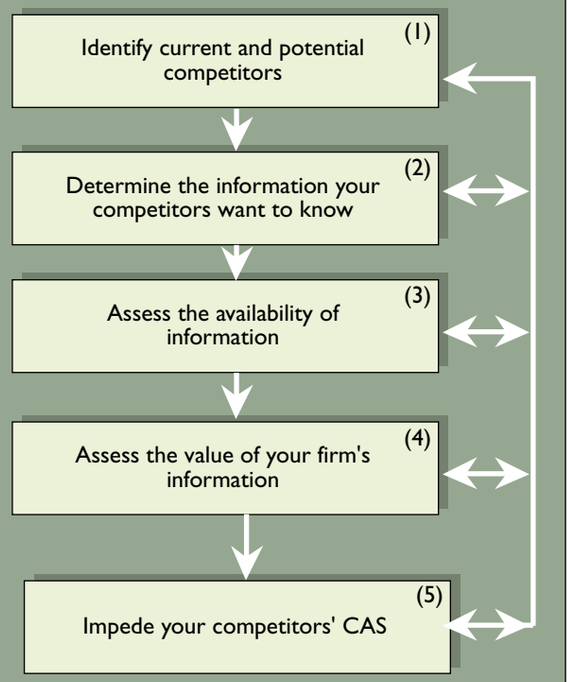
considered the logical game-theoretic response to CAS. Literature on CAS has not specifically addressed this game-theoretic issue. This is surprising because the CA literature has long since recognized the importance of the gaming aspects of competitive responses to such traditional concerns as competitors' pricing strategies [2]. It is also surprising the burgeoning literature on information security has not considered the recent developments relating to CAS as a security threat. Instead, the information security literature has concentrated on such issues as encryption, viruses, software and hardware controls (for example, [3, 7, 8, 10]).

Much of the effort related to these issues has been directed toward preventing illegal penetration of information. Yet, a major security threat (in terms of potential economic loss) to most organizations is the threat posed by the perfectly legal development of CAS by rival firms. Recent advances in applying data mining techniques to analyze massive publicly available databases has rapidly exacerbated this potential threat.

The main argument provided here is that firms need to view their competitors' efforts to make them part of a CAS as an important information security threat. Figure 1 provides a framework for considering information security as a response to CAS. The left-hand side of Figure 1 illustrates the CAS part of our framework. As shown in this portion of the figure, the development of a CAS involves searching for information on those firms viewed as the competition.[1] The ultimate goal is to develop a database on competitors for the purpose of gaining a competitive edge. Achievement of this goal is based on gathering information from unprotected information sources, as shown in the center of Figure 1. These unprotected sources, many of which are found on the Internet, include public databases, news media, commercial advertisements, and conversations in public meeting places. Creative techniques, such as data mining, can be utilized to analyze the information gathered.

The right-hand side of Figure 1 illustrates the information security part of our framework. This side of the figure highlights the fact that a corporation intentionally puts part of its databases into the public domain. This information may include, but not necessarily be limited to, information in public databases due to regulatory requirements (for example, annual financial reports). Another part of the firm's databases will be regarded as highly confidential and strong efforts to protect such information from any outsiders will be made. Somewhere in between these two extremes will be information accessible to corporate partners, but not intended for public consumption. As

Figure 2. CAS defense plan.



[1]For purposes of this article, it is assumed that only legal and ethical means of acquiring information on competitors are utilized.

indicated by the intersecting components of each separate database, there are overlapping aspects to the individual databases.

The right-hand side of the figure makes it clear that some aspects of a corporation's databases are readily accessible to competitors for their CAS. However, this side of Figure 1 is also intended to indicate that proper use of firewalls can impede a firm from becoming an unintentional part of its competitions' CAS. Keeping Figure 1 in mind, we turn to devising a plan for implementing information security as a response to CAS. This plan is our CAS defense.

CAS Defense

There are five steps to our CAS defense plan. Taken together, these steps are intended to impede, if not prevent, your firm from becoming a meaningful part of the competition's CAS. As we discuss each step depicted in Figure 2, it should be noted that the sequential nature of the discussion should not be interpreted to preclude an interactive process. Indeed, it is quite likely that each step will require the rethinking of previous steps.

Step 1. Identify current and potential competitors. Determining your firm's competitors is the first priority. Determining the firm's current competitors is reasonably straightforward. It essentially requires an assessment of the firm's current sales by industry and product line, and determining which firms compete in the same markets. However, determining a firm's potential competitors is far more complicated. Not only does your firm need to anticipate which firms might move into your existing markets (through expansions, mergers, and so on), but your firm also needs to consider which new markets it plans to enter (again, through expansions, mergers, and so on). One way or the other, the objective is to determine which firms might want information on your firm.

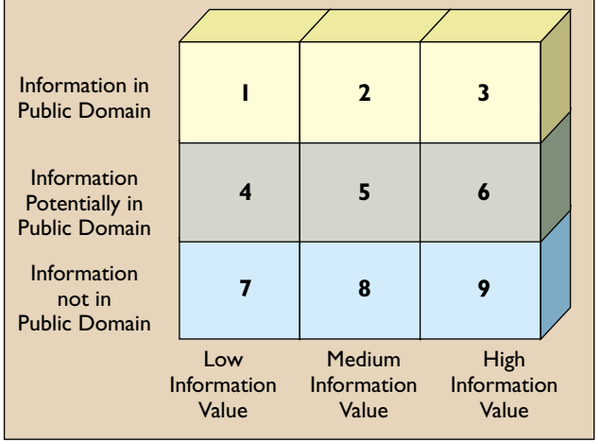
Step 2. Determine the information your competitors want to know. Once your competitors have been identified, the next move is to determine the type of information about your firm that competitors would find most beneficial to include in their CAS. In pursuing this step, a logical place to begin is to think in terms of market position data. Competitors usually want information on your firm's market share, product prices, pricing strategies, new product developments, and potential mergers and acquisitions. Information related to performance data is another natural area to consider. Competitors usually want information about your firm's profits, cost structure, return on assets, residual income, and margin of safety. A good way to approach this step in the CAS defense plan is to think about the type of information you would want to know about your competitors.

Step 3. Assess the availability of information. A crucial defensive measure is to assess where and how the competition can acquire the desired information previously identified. In terms of specific sources of data, a firm can develop their CAS based on publicly available data (for example, SEC required filings, popular news media clippings, industry publications, and published financial statements) as well as product tear-down data (firms often have the competitors' products torn apart and analyzed).[2] To carry out this step, it is useful to develop a continuum of information availability. The continuum could range from information absolutely not in the public domain (for example, information on secret formulas) to information that is absolutely in the public domain (for example, financial data filed with the SEC). Somewhere in the middle will be information potentially in the public domain, such as information your competitors can obtain through creative analysis or gathering of publicly available data. For example, by applying data mining techniques to the reams of publicly available data, the CAS group of a firm could assess patterns your firm did not intentionally put into the public domain (for example, the cost structure of some of your products, and your firm's margin of safety).

Once your competitors have been identified, the next move is to determine the type of information about your firm that competitors would find most beneficial.

[2]Although beyond the scope of this article, to the extent that illegal and/or unethical means of acquiring information about your firm may be used by competitors, standard information security mechanisms (for example, firewalls, encryption, software and hardware controls) need to be in place.

Figure 3. Public domain-value grid.



Overhearing private conversations in a public forum (for example, at a restaurant, during professional meetings, or in an airport) would be an example of creative gathering of information in the public domain.

Step 4. Assess the value of your firm's information. Determine the value of your firm's information to competitors, assuming it falls into the hands of your competitors. Of course, assigning an exact dollar value to competitively sensitive information is next to impossible. Such information can be used in a multitude of ways by a large variety of existing and potential competitors. However, a useful approach in this regard is to develop a three-tier classification scheme of information value.

The top tier would consist of information considered so highly valuable to competitors (and extremely damaging to your firm if competitors gain access to this information) that your firm is willing to spend huge sums of money to protect it from getting into the hands of competitors. Secret formulas, confidential plans regarding strategic mergers and acquisitions, and information on new product testing results are among the items likely to fall into this category.[3] At the other end of the spectrum, the bottom tier would consist of information viewed as having so little value to your competitors that your firm is not willing to spend any significant amount to protect it. Information on dress codes, annual retirement dinners, and starting salaries for clerical help are among the items likely to fall into this category. The center tier would consist of information deemed of medium value to your competitors, but clearly worth protecting. Information on the cost structure of your firm's products, pricing strategies, and financing decisions would fall into this category.

Step 5. Impeding your competitors' CAS. The final step in our plan is to devise a strategy for preventing your firm from becoming a meaningful part of your competitors' CAS. This strategy should pull together what was done in the first four steps. The objective is to prioritize such information in terms of information security efforts to protect it. In other words, since it is too costly to protect all information at a total level of security, your firm needs to assess where to invest its information security dollars in protecting competitively sensitive information. One way to do this is illustrated in Figure 3, which we call a "public domain-value grid." The specific information you believe the competition is interested in acquiring (steps 1 and 2) needs to be listed and placed in the appropriate cell. The listing of the various information items should be accomplished in consultation with various groups within the firm. For example, the management accounting/finance staff, the business strategy group, and the chief operating officer of the firm should be among those consulted in developing this list. The procedure for determining in which cell of Figure 3 to place the specific information is based on the two-way classification grid of information availability, in terms of the degree to which the information is in the public domain (Step 3), and the value of the information (Step 4).

A key aspect of Figure 3 is it highlights the fact information value and the degree of information availability are two independent, but interactive, dimensions of information sought by competitors. As such, the figure makes it clear that competitively valuable information, which is squarely in the public domain (information falling into cells 1, 2, and 3), cannot be protected (for example, information on earnings filed with the SEC). Thus, there is no gain to be derived from spending funds on protecting information falling into this category, regardless of the information value. Figure 3 also makes it clear that some information is of such low value to your competitors it is not worth spending much to protect it, even though it is not in the public domain (information falling into cells 1, 4, and 7 in Figure 3). In other words, Figure 3 presents a pictorial view that can help a firm decide where it can get the "biggest bang for the buck" in terms of securing competitively sensitive information. Most firms are likely to get the greatest payoff (in a cost/benefit sense) by investing in information security to protect items falling into cells 5, 6, 8, and 9.

Once a decision is made as to which information

[3]There are, of course, other types of information that may not be of great value to your competitors, but that your firm must keep secure for legal reasons (for example, employee health records). However, since the focus of this article is on protecting information of value to your competitors in a business sense, security considerations of these latter types of information are not addressed.

items should be the focus of information security, a strategy for securing such information is needed. The strategy recommended here is to avoid, confuse, and track, or ACT. The first part of the ACT strategy is to avoid placing the competitively sensitive information in the public domain to whatever extent possible. The use of firewalls, as depicted in Figure 1, is one way to accomplish this goal. Other, less direct methods should also be employed to avoid placing competitively sensitive information into the public domain. For example, during various corporate press releases, care should be taken not to give out unintentional sound bites related to cost structure, new product developments, and/or potential mergers.[4] Of course, there is a trade-off to consider in terms of the value of voluntary disclosure and the cost of competitors knowing about your firm's plans.

The second part of the ACT strategy is to confuse the competition. For example, when placing information into the public domain, it is rational to provide some confusing, if not outright garbled, signals to derail competitors from piecing together competitively sensitive information from various sound bites. Of course, there is a trade-off that needs to be considered between the market value to your firm from accurate signals about future growth opportunities and the cost of competitors knowing about such opportunities.

The third part of the ACT strategy is to track information inquiries concerning your firm made by your competitors. Via domain-name identification, a firm's Web site can instantly determine the origin of an inquiry. Such tracking could take several forms, including the number of hits to your Internet site by individual competitors and a breakdown of the actual information viewed. One purpose of this tracking is to make your firm aware of, and sensitive to, the kinds of information your competitors are interested in gathering on your firm. Another purpose would be to employ Web-access blocking so as to prevent certain competitors from entering your firm's Web site.

One way or the other, firms need to face the fact there is a gaming aspect to competitor analysis systems. Information security is the logical response in such a game. Although not a panacea, the CAS defense plan can go a long way in impeding, if not preventing, your firm from becoming a meaningful part of a rival's CAS.

Conclusion

It is well documented that firms are developing CAS. These systems gather and analyze competitively sensitive information about rival firms, with the goal of gaining a competitive edge. Since literature has not addressed how firms should respond to CAS, our objective here was to argue that the appropriate rival response to CAS is information security. A second objective was to argue that using information security as a response to CAS is logically thought of as the five-step CAS defense plan.

A fundamental premise underlying our defense plan is that the cost/benefit aspects of information security prevent firms from making all information completely secure. Accordingly, our CAS defense plan included a public domain-value grid as a means for determining where investments in information security can get the most value. In addition, our plan discusses a three-prong strategy for implementing such security. We believe the CAS defense plan discussed here can provide significant value to many, if not most, firms. Anecdotal evidence gathered by the authors seems to support this argument. C

[4]The term "sound bites" is used here to mean small bits of information, bits which alone have no apparent competitive value. However, through such techniques as data mining, numerous bits of information could combine to have significant competitive value.

References

1. Chen, M.J. Competitor analysis and interfirm rivalry: Toward a theoretical integration. *Acad. Manage. Review 21*, 1 (1996), 100–134.
2. Chen, M.J., Smith, K.G., and Grimm, K. Action characteristics as predictors of competitive responses. *Manage. Sci. 38* (1992), 439–455.
3. Denning, D., and Branstad, D. A taxonomy of key escrow encryption systems. *Comm ACM 39*, 3 (March 1996), 34–40.
4. Ghoshal, S., and Kim, S.K. Building effective intelligence systems for competitive advantage. *Sloan Manage. Rev. 28* (1986), 49–58.
5. Ghoshal, S., and Westney, D.E. Organizing competitor analysis systems. *Strategic Manage. J. 12* (1991), 17–31.
6. Guilding, C. Competitor-Focused Accounting: An Exploratory Note. *Accounting, Organizations and Society 24*, 1999, pp. 583–595.
7. Peyravian, M., Roginsky, A., and Zunic, N. Hash-based encryption. *Computers & Security 18*, 4 (1999), 345–350.
8. Pfleeger, C. *Security in Computing* (2nd ed.). Prentice-Hall, Englewood, NJ, 1997.
9. Porter, M.E. *Competitive Strategy: Techniques for Analyzing Industries and Competitors*. Free Press, New York, NY, 1980.
10. Simmons, G. Cryptanalysis and protocol failures. *Comm. ACM 37*, 11 (Nov. 1994), 56–64.
11. Young, M.A. Sources of competitive data for the management strategist. *Strategic Manage. J. 10* (1987), 285–293.
12. Zajac, E.J., and Bazerman, M.H. Blind spots in industry and competitor analysis: Implications of interfirm (MIS) perceptions for strategic decisions. *Acad. Manage. Rev. 16* (1991), 37–56.

Lawrence A. Gordon (lgordon@rhsmith.umd.edu) is the Ernst & Young Alumni Professor of Managerial Accounting and Director of the Ph.D. Program at The Robert H. Smith School of Business at the University of Maryland, College Park, MD.
Martin P. Loeb (mloeb@rhsmith.umd.edu) is a professor of accounting and a Deloitte & Touche Faculty Fellow at The Robert H. Smith School of Business at the University of Maryland, College Park, MD.

This project was supported by a summer research grant from The Robert H. Smith School of Business.