ASSEMBLING COMPETITIVE INTELLIGENCE USING CLASSROOM SCENARIOS

Helen L. Armstrong and John Davey
School of Information Systems, Curtin University of Technology, Perth, Australia, email: armstroh@cbs.curtin.edu.au

Defence Security Authority, Department of Defence, Canberra, Australia, Adjunct Research Fellow, Edith Cowan University, Perth Australia, email: jack.davey@defence.gov.edu

Abstract: This paper describes a scenario carried out in an intensive course in competitive intelligence and cyberwarfare. The scenario features two business organizations in tight competition and is designed to run over two days. The paper provides details of the scenario and discusses its application as part of a Master of Internet Security Management at Curtin University.

Key words: competitive intelligence, business intelligence, postgraduate education, and educational scenarios

1. INTRODUCTION

Competitive intelligence is not a new concept; numerous high-profile corporations have used it for decades. In order to survive, excel and outstrip rivals an organization must have an intricate knowledge of their own business, the industry and their competitors. The growth in awareness of competitive intelligence is evidenced by the growing number of publications describing how to establish a competitive intelligence department within an organization and how to carry out such a department's functions.

Competitive intelligence is undertaken in many different forms in both public and private organizations. Miller (2000) suggests that government agencies conduct intelligence focused more on threats than on opportunities, but in corporations this situation is reversed, with emphasis more on

C. Irvine et al. (eds.), *Security Education and Critical Infrastructures*

opportunities than threats. Shake and Gembicki (1999) suggest modern business executives are equipped with tools of combat with well appointed fortresses where information warfare in a business context involves achieving and maintaining an information advantage over competitors.

Competitive intelligence is seen as an essential part of the modern organization just as Sun-Tsu considered it an essential part of warfare strategy in 400BC. It incorporates both intelligence (analyzing gathered data about rivals) and counterintelligence (protecting ones own information sources). Intelligence is not confined to the military domain, and Kanaher (1998) suggests it is imperative to corporate organizations due to the rapid pace of business, information overload, increased global competition from new competitors, more aggressive competition, rapid technological change and forceful global changes in international trade agreements. The race to survive in a cutthroat global marketplace is on. Jones recommends every morning you ask 'what can I do to beat Company Z today' as neither your competition nor technology will wait for you (Jones et al., 2002). Competitive intelligence is as important as a good marketing department and has emerged as a 'must-have tactical tool' in the corporate world (Thomas, 1998).

The heightened awareness of competitive intelligence has been spirited by increased global competitiveness characterized by increased industry consolidation and fragmentation (Fleisher & Blenkhorn, 2001). The Internet provides both the data and tools for competitive intelligence, offering a wealth of information and search bots for those wishing to gather information about corporations and individuals.

Although competitive intelligence is not a recent phenomenon in the business community and awareness of the benefits of competitive intelligence to organizations is evident, the tertiary education industry has been chided for lack of response to this need. Fleisher and Blenkhorn (2001) state that competitive intelligence is rarely included in MBA programs, and Shaker and Gembicki (1999) believe competitive intelligence is an essential ingredient to effective management and state a manager's knowledge is derived from both formal and information education. They go on to suggest that the IT culture at large and education programs, at the Masters level in particular, neglect the area of competitive intelligence.

2. BACKGROUND

The unit of study presented is titled Business Intelligence and Cyberwarfare and is primarily a unit covering intelligence, competitive intelligence and corporate information warfare strategy formulation and

response. The unit is included in several Masters programs within the School of Information Systems at Curtin University, but is primarily undertaken by students enrolled in the Masters of Internet Security Management. Students require pre-requisite knowledge in Internet security and network architecture to enroll in the business intelligence unit.

The overall objective of the unit relating to competitive intelligence is to develop in students an understanding of the nature of business intelligence and its purpose in contemporary business environments. The unit encompasses both competitive intelligence and cyberwarfare and the topics covered include the competitive business environment, asset evaluation and identification, information systems and networking, intelligence and counterintelligence, information collection and analysis methods, counterintelligence by deception and denial of service, conflict in cyberspace, information systems protective security, insider system attacks, external system attacks, intrusion detection, incident reporting and situational awareness, reaction to attack, damage control and business continuity, national infrastructure issues and practical use of hacking and intrusion detection software tools.

The unit is conducted as an intensive course over two consecutive weekends. The unit is very practical in nature with the classes conducted in laboratories and small tutorial rooms. Students use the Internet to collect intelligence about organizations and then form groups to devise business strategies based upon given information and questions. Students are given a warm-up exercise, an actual case of sabotage in industry, to investigate. The students work in pairs and are required to answer a number of questions relating to the incident. The final part of the exercise is to take on the mindset of the saboteur and identify ways the perpetrator could have caused more damage. Their ideas are then shared with the class. In summing up salient points of the exercise, a number of questions are asked of the group, including "What does your partner now know about the way you think?", "How much information are you now willing to share with your partner?", and "How well could your partner or the rest of the group predict your action or reaction to a given situation based upon the knowledge they now have about the way you think?". The main objectives of this exercise are not only to use some tools for gathering intelligence, but also to raise students' awareness of the confidential nature of information and the way information can be used.

One of the most effective tools used in the teaching of this unit was a scenario carried out over two of the four days. The scenario featured two organizations competing for government funding and contracts in a high-tech industry. Each student was assigned either a management or technical role in one of the two organizations. In an effort to encourage all students to

fully participate the senior management roles were assigned by the lecturer to specific students. Experience has shown that the majority of classes contain a few natural leaders who dominate and take control rather than capitalizing on talents hidden in the more reserved students.

3. THE SCENARIO

Two organizations are competing for a government contract to build the rockets to launch communications satellites. Each organization is to build a prototype and the government will decide the successful product. Immense government funding has been made available to both organizations for the development of their prototypes. The two organizations are in a highly competitive situation and in order to survive, need to develop a leading edge over their rival. This requires gathering information regarding the activities of the other, turning it into intelligence, and devising strategies to gain a leading edge.

The overall aim of running the scenario is to allow students to apply methods of intelligence gathering, design competitive intelligence strategies and learn from the human interaction.

3.1 Phase 1

The aim of this phase is for students to devise strategies for gathering information about their rival and determine not only the short and long-term impact of their actions, but also the ethical considerations. They must also devise appropriate counterintelligence measures to ensure their competitor does not gather information about them.

Students are assigned to one of the two organizations. Management roles are allocated to members of the group, with about half the group assigned engineer and technician roles. Management roles assigned should include (as a minimum) the Managing Director, the CEO, Engineering Director and Financial Director for each organization. In both organizations the CEO is the driving force within the organization with power over resources and decision-making. The CEO advises the Managing Director who puts the stamp of approval on decisions following advice from the CEO. Before making decisions, the CEO consults the other Directors for information and advice.

Students are advised that the level of competition between the two organizations is very high as both are competing for the same government contract. Each organization needs to gather intelligence about the other, and

implement counterintelligence measures to ensure their competitor does not gather information about them.

Prior to commencement of the scenario activity, two appropriate students are separately approached to take on the roles of spies for the competition. The first spy works for Organization A but is having a secret affair with the CEO of Organization B and passing on confidential information. The second spy is an engineer employed within Organization B and is passing on selected information and data directly to the CEO of Organization A for a handsome fee. The CEOs are aware of the spy working for them, but not aware of the spy within their own organization.

The main activity in this phase is for each group to meet and decide what intelligence and counterintelligence measures they will implement. An opportunity for the spies to transfer information must be included at this stage, either a coffee break or end of the day's proceedings.

3.2 Phase 2

This phase covers a change in government funding for the project and the effect this has upon the two organizations. With cuts in funding both organizations must devise and produce a plan to reduce costs while still remaining the leader in the research and development.

After an election, the opposition political party takes power. The CEOs of the two organizations are called to separate meetings with the Chief of the Government agency handling the research and development grants (one of the academic staff) and are advised that the new government has decided to cut back on funding for the project. The CEOs are informed that their prototype should no longer require the same amount of initial funding as the majority of the research and development work should be close to completed, leaving only the testing to carry out. In effect, the funding available for engineering and technical research has been more than halved. Leaked information from the government agency regarding the proposed reduction in funding and proposed massive job losses reaches the media and hits headlines of the major financial newspaper.

The Financial Directors are given information showing that salaries are by far the greatest cost to the organization, particularly salaries for the engineers and technicians. Raw materials and overheads are insignificant in comparison to the salary costs. In order to complete the prototype they must use the available funds to purchase the remaining required raw materials, complete assembling the product and carry out launching tests. The CEOs are advised to gather information and opinions from their respective Directors and devise a course of action. As it is now the beginning of June, the new government funding arrangements come into effect in July, one

month's time. While the Directors are meeting, the engineers and technicians are given the newspaper article to read.

A plan of action must be decided upon by the management of both organizations, however, before this plan can be communicated to employees, the scenario moves to phase 3.

3.3 Phase 3

The aim of this phase is to highlight the use of perception management and its effect on a competitive situation, and the role uncertainty plays in the actions of individuals. Given the information contained in the press article, engineers and technicians are now uncertain of the status of their jobs. An opportunity is given to employees to mix with their rivals and colleagues at an industry function. This presents the staff with an opportunity to solicit information about the competitor, transfer confidential information by informants, or to develop potential employment opportunities in case they are retrenched.

The new government has redesigned the government portfolios and established a new agency to handle ITC (information technology and communications). To market this event the government has sent invitations to attend a promotional seminar to all employees in the industry, including all employees of the two organizations involved. Coffee and cake is provided and open networking between professionals in the industry is encouraged.

After completing their action plan in phase 2, the CEOs must now meet with their staff and inform them of the government funding decision and the management's resultant action plan. The obvious course of action is to retrench a sizeable number of engineers and technicians. After considering the plan of action presented by the respective CEOs, the engineers and technicians in each organization meet and decide their course of action, and report back to their management.

3.4 Phase 4

The aim of the final phase is to share information, strategies, and to develop a big picture of the situation. The two groups join in the classroom and present their intelligence and counterintelligence strategies, and their action plans for the funding cuts. The engineers and technicians discuss their reactions to the management plans. In concluding the exercise, the spy employed by Organization A makes a confession, stating they regret the affair and trust it will not effect their respective marriages. The informant employed by Organization B also confesses.

As a final exercise, students are requested to reflect upon the exercise, and write a report on what they learned about themselves, the situation, and the methods they used in the scenario. This final exercise supports an action learning approach where reflection consolidates the learning process by evaluating strategies and tools. In addition, it allows the student to reflect upon their own thinking and the impact of their actions as well as that of others involved.

4. APPLYING THE SCENARIO

The aim of the scenario was to apply some of the information on intelligence and counterintelligence the students had read from books and articles or covered in lectures and to give the students some insight into the complexity of their application, by people, in an organizational setting.

The scenario was run for the first time in the second semester of 2002. The phases of the scenario were carried out over two days, allowing the students to make notes, consider strategies and develop ideas away from the classroom. There were 26 students enrolled in the unit, from a variety of backgrounds and nationalities. Many of the students, particularly those from Asian countries studying full-time in Perth, had little or no IT business experience. It was noted that those with business experience tended to be more outspoken.

The intelligence and counterintelligence strategies developed by the two groups contained not only the usual intelligence gathering techniques, but also a few 'off-the-wall' suggestions bordering on the unethical. Some examples included causing physical harm to key employees of the rival organization, infiltrating the rival organization (cleaning staff, maintenance technicians, etc), hacking into the opposition's computer networks and not only copying information but also modifying engineering formulae and counterfeiting data in order to sabotage the product development.

The reactions of students to given situations as the scenario unfolded would have been an interesting study in culture and ethics. For example, after a few of the engineers employed by Organization A became aware of the funding cuts and threats to their jobs they approached management employees of Organization B at the ITC industry seminar, offering services and confidential information about intelligence and counterintelligence activities. Engineers employed by Organization B approached a few of the directors and engineers of Organization A and proposed a merger.

The engineers from Organization B offered to work for little or no pay until the contract was awarded by the government agency in the hope that they would retain their jobs in the long term. When the CEO of Organization

B was asked if she would give up her BMW corporate vehicle to assist payment of the engineers' salaries, she adamantly refused and became quite upset. She admitted she would rather leave the organization than give up her status symbol.

As is often the case in group exercises, one or two members of the group become dominant with opinions and suggestions. The group of directors for Organization A contained two such students, who regularly tried to coerce other members of the group, or take control and implement actions without due consideration of consequences. As the exercise progressed the proposed actions became more radical and unethical, and the reserved members of the group gradually became more outspoken in their opposition to these suggestions.

The feedback from the students was very positive, with all students stating they learned significantly from the scenario, particularly regarding intelligence, counterintelligence, strategy, security and many lessons in human relationships. The university carries out a student evaluation of units conducted, seeking feedback on the learning and academic value of the unit, instructor enthusiasm, individual rapport, grading, comparison with other classes, lecturer rating, organization and clarity, breadth of coverage, and group interaction. The ratings for all these factors exceeded the university norms.

5. CONCLUSION

The scenario described above proved to be an interesting and effective means of applying much of the intelligence and counterintelligence theory taught in the lectures and textbook. Students were able to apply this theory in an interesting and challenging situation, being supported by the learning environment.

The scenario enabled the teaching objectives for the competitive intelligence elements of the course to be met, and students found the exercise to be of great academic value. Students also valued and learned from the group interaction. Not only were they able to devise strategies and partially apply them, but were also made aware of the complexities and constraints of a real-world environment. Other than those who had been told prior to commencement of the scenario, none of the students were aware of the informants in either group, and no procedures for internal checking were included in the intelligence and counterintelligence strategies.

In addition, the scenario prompted students to consider the impact and the ethics of their actions. The building of the big picture by sharing information and feelings at the end of the exercise allowed students to see the holistic

view and how their actions affected others. The final activity involving reflecting upon what had been learned, not only in the application of theoretical concepts but also in human thinking and interaction.

REFERENCES

Fleisher, C.S. & Blenkhorn, D.L., 2001, *Managing Frontiers in Competitive Intelligence*, Quorum Books, Connecticut, USA

Jones, A., Kovacich, G.L. & Luzwick, P.G., 2002, *Global Information Warfare: How Businesses, Governments and Others Achieve Objectives and Attain Competitive Advantages*, Auerbach Publications, Washington DC, USA

Kahaner, L., 1998, *Competitive Intelligence*, Touchstone Books, New York, USA

Miller, J.P., 2000, *Millennium Intelligence: Understanding and Conducting Competitive Intelligence in the Digital Age*, Cyberage Books, New Jersey, USA

Shaker, S.M. and Gembicki, M.P., 1999, *The WarRoom Guide to Competitive Intelligence*, McGraw-Hill, New York, USA

Thomas, J., 1998, Intelligent Intelligence, *The Wall Street Journal*, December 7, No. 29