Chapter 3

The Role of Security and the Security Manager in Mergers and Acquisitions

Every battle is won before it is ever fought. – Sun-tzu, The Art of War.
Quoted by Gordon Gekko in the movie Wall Street

INTRODUCTION

This chapter addresses why security is important to the process of mergers and acquisitions. We examine the most relevant security issues and concerns a merger and/or acquisition team encounters and why having a security professional as part of the team is essential to effectively resolving security issues, addressing security concerns, and applying appropriate security controls.

The security manager or their professional representative serves as a consultant to the merger and acquisition team, providing guidance and direction for all security matters. In essence, they are the merger or acquisition team's subject matter "expert" for all issues of security. In addition to the security consulting role, the security manager or professional also fulfills the role of a department or function manager responsible for directing and managing all security department-related activities in support of the team and the overall effort. The role of department or function heads is similar to the role of any other function lead on the merger and acquisition team. Each is responsible to ensure they manage all activities supporting the merger or acquisition related to their specific discipline and department; for example, the manager of finance ensures that all financial matters are properly handled by his or her organization just as the manager of facilities manages all relevant facilities issues.

Support from security for the merger or acquisition effort can be divided into two phases:

- Premerger support
- Postmerger support (see Figure 3.1)

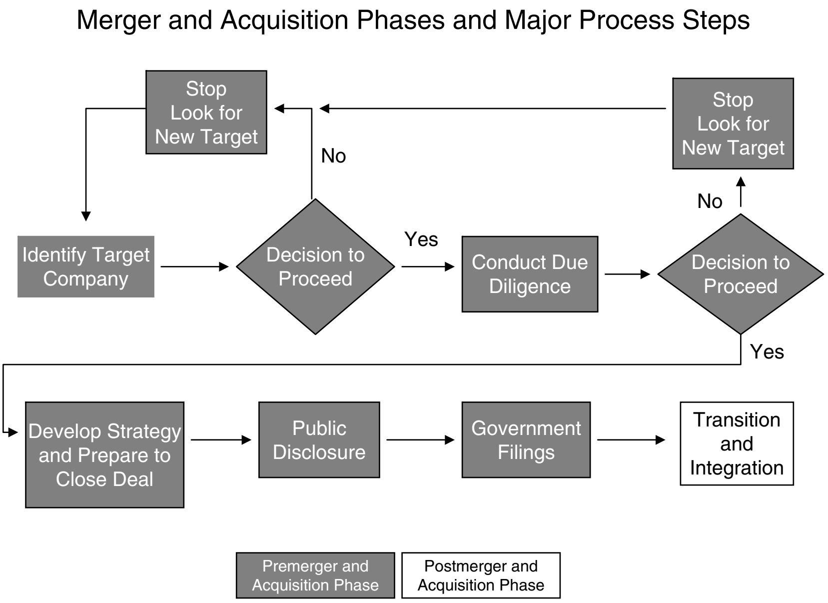

Figure 3.1 The phases and major steps of a merger or acquisition.

Furthermore, the contribution security makes to the entire effort can be further segmented into the following three categories:

- Protecting the effort itself: Security measures are applied to the merger or acquisition effort to ensure that it is properly protected. That includes the implementation of measures to protect the confidentiality of the effort and its people, information, and physical assets.
- Providing subject matter expertise: The security manager or professional serves as a member of the team and provides guidance, direction, and consultation on all security-related issues and concerns.
- Evaluating the security condition of the target company: The security manager is charged with assessing the security condition of the target company. Here the security manager conducts a security audit[1] of the target company's security program and overall security condition. That becomes part of the total team's assessment. Any issues identified are given consideration in terms of their effect on closing the deal.

[1] The term *security audit* as used here does not mean the same as an audit for compliance, as would be done by the auditing staff. In this context, it is an evaluation as to the asset protection measures in place; how they compare to that of the acquiring company; what must be done to bring them up to acquiring company asset protection standards; and what best practices they have in place and should be adopted by the acquiring company. In addition, the costs involved in this integration effort should be identified and added to the overall cost of the merger or acquisition.

Executing mergers and acquisitions usually requires a great amount of time and effort. Transactions can be costly and complex. Merger and acquisition teams engage in deals that shape the strategic direction of a company, some only slightly; others may cause a major change in the way a company operates. In any type of merger or acquisition, the acquiring company's security organization has an important role to play in this process. Security needs to be an active member of the merger and acquisition team from the start.[2] From the initial decision to pursue a target company, to the start of a due diligence effort, and right through the integration of the newly acquired or merged business, security has a role.

Merger and acquisition teams have a great deal of responsibility. The deals they make may bring great value to a company. If not executed properly, they could be a disaster. To be effective, the merger and acquisition team must be highly skilled in many disciplines. Furthermore, team members must work well together under stressful and sometimes adverse conditions. Mergers and acquisitions bring much external attention and interest to companies, and not all of it is positive. Highly experienced and skilled teams with proper cross-functional representation are best suited to manage this process. Furthermore, merger and acquisition (or divestiture) teams must operate within well-defined boundaries following established processes. These boundaries and processes must be institutionalized within a company charter.

Sample Charter for Executing Mergers, Acquisitions, and Divestitures

Our Company pursues mergers, acquisitions, and divestitures when such transactions will promote long-term growth in value for our shareholders. The Senior Executive for Business Strategy is responsible for providing strategic analysis and guidance for the development of long-range business strategies. When these strategies involve mergers, acquisitions, or divestitures, this position is responsible for the following actions:

- *Identify candidate target companies or business units for merger, acquisition, or divestiture*
- *Conduct initial analysis of each target's potential strategic and financial value to company*
- *Lead all due diligence activities ensuring the due diligence team identifies all issues and risks associated with any potential merger, acquisition, or divestiture.*
- *Provide valuation guidance for all mergers, acquisitions, and divestitures*
- *Make final assessment and recommendation for all potential mergers, acquisitions, and divestitures to the company CEO*

[2] http://www.csoonline.com/read/030103/mix.html CSO Magazine, March 2003

Mergers and acquisitions are complicated business transactions[3]. They become even more complicated when conducted internationally. In this post-September 11, 2001[4] world, issues given little or no consideration before the attack on the United States by international terrorists now must be considered. Conducting business in the Middle East became much more dangerous and problematic immediately after the events of September 11 and more so during the conflict in Iraq.

In a merger or acquisition, if the acquiring company is a U.S.- or European-based company, it must be concerned with laws, many of them recently enacted, prohibiting doing business in any way with other companies and countries that may be involved with sponsoring terrorism. Western companies are also faced with restrictions on sharing or transferring certain types of technologies, in particular, technologies with the potential for military application or technologies that can be used in the development or production of weapons of mass destruction.

At the very least, these restrictions create limitations on the exchange of information between an acquiring company and the target company. Limits on obtaining information may limit what one company can learn about the other. That in turn may affect the ability of the acquiring company to accurately value the target company. Knowing the extent of these restrictions beforehand will help to better understand what the union of the two companies will and will not create.

Process Steps for Executing Mergers, Acquisitions, and Divestitures

The transaction stages of any merger, acquisition, or divestiture occur in the following order:

1. *Identify the target for its strategic fit and financial impact to acquiring company based on a review of public data.*
2. *Make a recommendation to investigate when the results of the identification stage reveal a good strategic fit or other potential benefit to acquiring company.*
3. *Conduct a due diligence by establishing a team to determine the value of the target company. The team must review all aspects of*

---

[3] Determining the value of a company is a complicated process. To learn more about value, value-based management, and the process of valuation, the reader should consult other publications on valuation produced by companies involved in such matters.

[4] Reference to the post-September 11, 2001 world is made to highlight the change in global security conditions as a result of the acts of terror perpetrated on the United States. On this day, terrorists crashed airplanes into the World Trade Center in New York City and the Pentagon in Northern Virginia. More than 3000 people perished during these acts of terror, which were shortly followed by an American led "war on terrorism" and invasion of Iraq. This series of events created what many referred to as a "new normal" condition. This is to suggest that the safety and security of peoples all over the world will not be the same for years to come.

the target business and prepare a formal assessment including risk identification and the impact of all observations and findings on the value of the target. This assessment should be delivered to the company CEO or the company Board of Directors.

4. *Based on the findings, a recommendation to proceed or not to proceed is made by the due diligence team to the CEO and/or to the Board of Directors.*
5. *Define parameters of a negotiation and implementation strategy that will result in closing the deal and the signing of a contract with the target.*
6. *Public disclosure (press release or announcement) of the transaction is made. This disclosure does not include release of competitive sensitive information, only the disclosure of the transaction.*
7. *Government filings must be made, as various legal filings are required to implement and authorize the transaction. The legal department, with support from the due diligence team, has the responsibility to submit all filings*
8. *Conduct an orderly transition of the target into or out of the company. A divestiture must be spun off from the company and an acquisition must be integrated into the company.*

The acquiring company's mergers and acquisition team generally looks to the legal department to handle such matters. However, it has been our experience that often the legal staff doesn't have a good understanding of all the applicable security-related laws, regulations, and restrictions. This is especially true if one is dealing with a merger or acquisition between companies of different countries.

The security professional should not expect the legal staff to be the sole provider of such information to the team. The security professional assigned to the team should be knowledgeable in such matters and coordinate that information with the legal staff. After all, for security professionals to successfully assist with the merger or acquisition, they must have a detailed knowledge of the applicable laws, regulations, and such so that they can formulate the asset protection integration with the least amount of chaos—and there is usually some chaos that takes place with a merger or acquisition.

Laws and regulations bring with them close government oversight. This oversight can be used as a tool to help navigate successfully through the legal and regulatory requirements. However, laws and regulations are not the only concerns a merger or acquisition team must deal with. There are a plethora of considerations that must be addressed by the merger and acquisition team. It is up to the team to sort out all issues early in the effort and to ensure that a skilled and experienced team is in place to work them.

Having a cross-functional team with representatives from all critical disciplines along with a well-defined game plan increases the probability of success. The security staff is often overlooked when it comes to establishing a merger or acquisition team. If not invited to join the team, the security professional has an obligation to get on that team.

WHY SECURITY?

The role of security within a company is to protect people, information, and physical assets and to mitigate risks to the company assets.

> ***Security:*** *The American Heritage Dictionary defines security as: Freedom from risk or danger or something that gives or assures safety.*

These are some questions that are often asked about security's role in a merger or acquisition:[5]

- Why does a merger or acquisition need security support?
- Aren't mergers and acquisitions just ordinary business transactions?
- They seem to occur nearly every day, so what is so special about them that they require special security support, or any security support at all?
- What value does a security professional bring to a merger and acquisition team?

A security professional involved in a merger or acquisition must be able to answer these questions as part of convincing a mergers or acquisition team that security should be an integral member of the team. If invited on the team when the team is first formed, the security professional must still be able to answer the preceding questions as part of the security operations plan that is needed to ensure the successful merger and integration of the acquired or merged company.

[5] Throughout this chapter and this rest of this book we will address these and many more questions concerning the need for security in support of mergers and acquisitions. We intend not only to provide answers but to provide a framework of understanding of how mergers and acquisitions work and why security plays such an important role in the success of these business transactions. Furthermore, we will provide a model to be used as a guideline for security professionals to assist them in their effort to provide security support. Use of this model is not intended to be exclusive to the security professional. We expect it to be useful for any member of a merger and acquisition team in helping them better understand the complexity of the many issues associated with mergers and acquisitions. It will also help in understanding basic and unique security-related issues and the necessity of having a security professional as part of the team.

If the business relationship is one of a merger, generally a joint merger team is formed; however, employees of one or the other of the companies must take a lead position. Regardless of whether or not the security professional is in a security leadership role or just a support member of the security team, it is important to understand the security issues and the role of security to the project.

Getting Started and How Security Can Help

Mergers and acquisitions are extremely important matters and have a major impact on any company. In some cases, mergers and acquisitions are so large and encompassing that they drive a complete transformation of the companies coming together and essentially cause the creation of a new company. An action of this nature is not something to be taken lightly. Moreover, it does not successfully occur on its own. Much planning and effort are needed to make a merger or acquisition a successful event. Many business disciplines must be part of the planning process. To achieve maximum success, all affected business disciplines must become part of the process. Security is not an exception. A security manager or security professional staff member must be part of the team from the very beginning. This means that from the early planning stages, the merger or acquisition team needs to be thinking about security and must have the support and input of a security professional.

As alluded to earlier, security professionals should know how mergers and acquisitions get started. Company executives consciously engage in a strategy to expand or improve the business. There are many options available for them to consider for expanding or growing the business. Mergers and acquisitions are but one and are generally the fastest way to achieve growth. A company will often establish a business team to seek merger or acquisition opportunities. Within these teams is where the ideas for potential target companies germinate. Merger and acquisition teams generally include members with expertise in business strategy, finance and investments, and executive management. They should also include a security representative.

A large company may have the luxury of maintaining a full-time team of professionals dedicated to mergers and acquisitions. A small company or a company with less experience in mergers and acquisitions cannot afford to have a full-time team, so it forms an integrated process team, drawing from within the company to look for merger or acquisition opportunities. Usually a team consists of business professionals from within the company, led by financial experts or strategic planners, and with some support from outside expertise.

Involving outside expertise is always a good idea if for no other reason than bringing in an independent perspective. Someone who is sufficiently disassociated from the business to bring an independent view will help balance the team's thinking and complement its expertise. It is not uncommon for a merger and acquisition team to want a merger so badly that its own desires cloud its ability to see any negative aspects to making the deal. Using outside expertise may help prevent this from occurring. Furthermore, hiring a consultant when little or no internal expertise exists within the company may be a prudent course of action.

After the core merger and acquisition team is formed, it begins its work to identify potential target companies for capture. It is in these very early stages of the planning when the security representative to the mergers or acquisitions team should be relied on to assist. As part of the effort to identify suitable target companies, the team does preliminary work to learn more about potential target companies. It is precisely in these early stages where security can begin to offer much support. Generally, at this stage of the process, security can provide investigative or research assistance to help the team learn as much about the target company as possible. This support is much like conducting a preemployment background check on a potential employee. In addition, this initial step can use the same processes used for competitive intelligence collection.

The security manager can conduct a similar assessment for a target company. By searching court records, security can learn if the target company and/or its key executives have any history of criminality. Moreover, information about the reputation of the company may be learned through information brokers and public records. This information, if learned early enough, may help facilitate an early assessment and possibly early decisions. For example, learning that a potential target company has a conviction for corruption may influence how the value of the target company is assessed. If the information reveals problems of a more serious magnitude, an early decision may be made to scrap the effort, thereby reducing the likelihood of wasting future time and effort or from causing any embarrassment to the acquiring company and its reputation. Moreover, learning something similar about a key executive may trigger a more thorough assessment of the company to be acquired in an attempt to ferret out as much information as possible, thereby supporting the merger and acquisition team objective to make the best informed business decisions.

Security in the early stages of the effort involves more than the quest for quality background information on potential target companies. The role of security and the security manager reaches far beyond conducting investigations. The next sections describe other areas that require attention and support from security professionals.

Protecting the Effort Itself: Use of Operational Security Methods

Protecting the effort is where security begins. It is the first concern for the security manager and should also be a high priority for the merger and acquisition team leadership. If the merger or acquisition effort itself is not properly protected, it may be damaged or derailed.

Security is a protective discipline. When supporting a merger or acquisition effort, that responsibility does not change. Nearly all members of the merger and acquisition team are focused on making the deal. Each team member conducts an assessment of the target company working within his/her area of expertise. Collectively, they come together to create a final assessment. During this process very few, if any, team members focus on protecting the effort. The security manager must provide the leadership and expertise necessary to apply an appropriate degree of protection to the effort. The security manager is responsible for ensuring that proper security controls are in place, all team members understand what the controls are and how to work within them, and why they are important. An uninformed team will not consciously comply with security requirements. An ignorant or apathetic team will just ignore them.

Protecting the effort generally breaks down into three areas:

1. *Confidentiality of effort:* Protecting the confidentiality of the effort is paramount. When seeking to make a major strategic move such as acquiring another company, it is not wise to expose these intentions too early. Exposure of intentions too soon could alert competitors, causing them to react in such a way as to prevent this transaction from happening. That could mean they seek to acquire the target company themselves, thus making the desired acquisition that much harder. Furthermore, if the market has an indication that a deal is developing, the stock price of the target company could rise. If it rises high enough, the increase in value could kill the deal. It may cause the price to acquire the target company to rise beyond what the acquiring company is willing to, or capable of, paying.

Maintaining confidentiality of a merger or acquisition, in its early stages, may be the most critical element of the effort to protect, but it sure can be argued that it is the most difficult. It is not a natural action for a team used to sharing information with each other to effectively stay within those boundaries and not share information, albeit limited, with others outside the team. Moreover, team activities and behavior, when observed by knowledgeable people, can be very revealing. Confidentiality further breaks down into two major considerations:

- Confidentiality of the total effort: Knowledge that the effort exists may need to be kept from everyone outside the merger and acquisition team. Disclosure of this information may compromise or jeopardize the effort. For competitive reasons, it may be necessary to keep the existence of the effort unknown to all but the merger or acquisition team itself. At some point in time, all mergers and acquisitions become known, but that occurrence must be controlled, deliberate, and approved by executive management. It must not be accidental or happenstance. In the event a company is proceeding down the path of a hostile takeover action, at least in the early stages of the process, the acquiring company may not want the targeted company made aware of these plans. If the target company does become aware of plans to acquire them and it is not interested in being acquired, it may have sufficient time to develop a variety of defensive measures to prevent itself from being acquired. Hostile takeovers make for very good drama. Keeping a low profile for as long as possible can help prevent or mitigate this distraction.

- Confidentiality of the team's work must be maintained: Even if it is publicly known that an acquisition team from one company is pursing a targeted company, there are still things that must remain confidential. Specific strategies, plans, processes, analysis, and assessments must not be revealed to people outside the team without the expressed permission of team leadership, or another in the executive management chain. Unauthorized releases may compromise or harm the effort. At the very least, unauthorized releases may provide a competitor with information (intelligence) it did not possess and did not have to work to get. This information may even assist a competitor in a countermove, thus preventing the merger or acquisition or at least making it a more difficult transaction. An unauthorized release of information may allow a competitor to gain information of value at little or no cost to itself. This is never a good situation.

The security professional must work with the team leader, and both must accept and share responsibility for leading the protection of the entire effort. Accepting responsibility is part of the process of accountability. Team members play an important role in protecting the effort. Each must be made to understand the need for confidentiality. Each must adhere to approved practices and engage in appropriate behavior to ensure confidentiality. The security professional is responsible for developing and implementing processes and procedures used by all to protect the effort. Periodic testing of these processes and procedures is essential to ensure they continue to work well and serve as they were intended in the effort to protect.

2. *Protection of information:* In some ways, information is what the merger and acquisition is all about, notwithstanding the fact that teams' overall objectives are to find the best targets for mergers and acquisitions, and to successfully execute those mergers or acquisitions, thereby bringing the intended value to the company. To do so

effectively requires obtaining and evaluating information. Information is the lifeblood of any merger or acquisition effort. It is information that is sought, obtained, synthesized, analyzed, and acted upon. If the information gathered does not have integrity (true as opposed to false or inappropriately manipulated) and confidentiality and is not available when needed, it loses value. If there is a single critical component of the effort requiring protection, it must be information.

3. *Protection of the merger and acquisition team:* Merger and acquisition teams also may require protection. Not all work is accomplished within the confines of the company office building. Often the team must venture out to accomplish its work. If the target of the merger and acquisition team is a foreign company, some or all of the team will need to visit that company to perform critical elements of their analysis.

In a high-profile event, team members may require protection as they conduct their business outside the confines of the company office. Competitors, media and special interest groups may desire to learn more about the activity and get close to team members. These contacts must be controlled and not allowed to occur randomly. In addition, if information is known to the public, such teams may be the target of national zealots who oppose the foreign merger or acquisition. Terrorists may also attempt to gain maximum publicity by violent acts targeting the team. Effectively applying protective measures is the role of security, often in coordination with local law enforcement agencies.

Assessing the Security Condition of the Target Company

Assessing the security condition of the target company is of utmost importance. After all, it is all about protecting the company's assets.

- *Assess the security condition of the target company:* The most capable and prepared person within the acquiring company to assess the security condition of the target company is the security manager. In the effort to learn and know as much about the target company as possible, the services of the security manager are required. The security manager must be an equal member of the team to be an effective member of the team. With this tasking, the security manager is much like any other team member. A specific function within the target company must be evaluated as part of the overall team assessment.

Knowing about security vulnerabilities and related issues early enables the merger and acquisition team to consider these factors as it makes an assessment of the target company and assigns a value to it.

Unless severe security problems exist, security issues generally never break the merger or acquisition (deal). However, security problems or a substandard company security program can impact the value of the deal. Anything that may affect the value of the deal must be given serious consideration. Failure to do so is something less than a proper due-diligence effort.

Like any other member of the team, the security manager must conduct a security assessment that is as thorough an evaluation as possible. Recognizing that there will be limits on time and the availability of information, the security professional should have a set of measurement tools to use to sort and evaluate the collected information. Obviously, this must be accomplished to make sense of what is learned and to communicate that back to team members as a meaningful set of information useful to the overall assessment.

In every instance the functional team makes an evaluation of the current condition of each function within the target company. Moreover, each team seeks to understand the future condition of each function and anticipate potential issues or problems in terms of how those issues and problems could possibly affect the future capability of the company.

- *Help move the effort along:* Speed and thoroughness are necessary but competing objectives. Moving too quickly may lead to mistakes or missed information. Moving too slowly may be costly in terms of lost time. As is the case with all business transactions; "time is money." Moving too slowly will also allow time for a competitor to learn more about what the acquiring company is planning. The security manager can and must help the effort move along. As the team proceeds through the merger or acquisition process, without doubt, issues or problems will develop. Some of these issues and problems have security implications or require security support for resolution. Being able to react quickly to security problems and issues by implementing effective measures or solutions will help keep the effort moving along as quickly as possible.
- *Identify synergies:* Much of the merger or acquisition team's effort is spent seeking to identity potential synergies that can be exploited during the integration phase and can lead to cost reductions, process improvements, or increased productivity. Most of this activity will occur after a merger or acquisition is made. However, to the extent possible, identifying potential synergies before deal closure provides an integration team with an advantage. If you recall, synergies are achieved when two companies bring different strengths together, enabling them to improve or eliminate existing weaknesses and maximize on their strengths. Capitalizing on synergies is critical to achieving cost savings, cost reductions and cost avoidance. Moreover, synergies will be sought as part of the effort to eliminate redundan-

cies. In the postmerger or acquisition phase, all staff in all company functions and disciplines will be expected to examine their organizations, seeking opportunities for synergies. Security is no exception. How security does business in the target company must be examined. When the two companies come together, performance improvements will be expected. Best practices of either company should be considered for adoption and poor practices slated for reengineering or elimination.

Preparing for the Integration of the Newly Acquired Company into the Acquiring Company

The security professional must prepare for the integration of the newly acquired company into the acquiring company.

Identify Security Requirements for the New Company

What will be the security needs of the new company? The combination of two companies into a single larger company changes that company in many ways. Those changes should be anticipated and evaluated in terms of future security requirements. Some of the security needs of the newly created company may be driven by the security condition of the two companies coming together. Any security problems or vulnerabilities identified during the assessment phase will require attention during the integration phase. Understanding the impact of security problems and vulnerabilities early on will allow more time for planning and development of mitigation measures.

In some cases when two companies come together, it may not be practical to simply impose the security practices of the acquiring company on the new company. The structure and operations of the new company may be so different from either heritage company that the overall security needs and requirements for the newly combined company may now differ significantly. If this is the case, much work will be needed in assessing and understanding those needs and developing procedures and practices to support them.

Controlling Rumors

Rumors are not a good thing, but without doubt they will develop fast and quickly spread. It is often the case that rumors contain a sufficient amount of truth to be at the very least annoying and perhaps even harmful. Some rumors may be more false than true; others will be more true than false. In any event, they are still rumors. Rumors can be complicated. They may involve teams of people to make them happen. As information is exchanged, rumors develop and anxiety levels soar. Rumors grow and spread fastest when little is known about an activity. People have a tendency to fill a knowledge void with supposition and their own conclusions, no matter how fantastic these conclusions may seem.

Preventing rumors is impossible. Limiting and controlling them are possible. Frequent, structured, honest, and planned communications will cut down on the development and spreading of rumors. For the overall effort, this is a concern. Security is no exception. Within the security organizations, security managers must work to communicate openly, honestly, and frequently to ensure that the proper messages and information are communicated, not allowing for rumors or other forms of misinformation to develop. Rumors heighten the already high sense of anxiety employees have resulting from situations of uncertainty. Controlling rumors will help mitigate that tendency of anxiety. Communicating often, openly, and honestly will help keep employees informed and their anxiety level low. Using operational security methods will help mitigate such problems. The team's security manager may want to consider an operational security umbrella to cover the acquisition or merger and using compartmentation, plan for "rumor control." In fact, at the initial phase of any merger or acquisition, the security manager should provide the team with a briefing on how to use operational security methods as a tool to help maintain confidentiality of the proposed merger or acquisition.

Global or International Aspects

If the merger or acquisition effort involves companies from different countries, the role of security becomes more involved and demanding. International travel, laws, and regulations from multiple countries and cultural and language differences along with differing business practices make the task of protecting the effort, people, and information more complicated. Having an understanding of international business issues will be helpful. Having a security manager on the team with experience in international business, and security will be invaluable to the effort. When an acquisition team leader selects a security manager to support the team, the leader should keep in mind the importance of international business experience.

THE ROLE OF THE SECURITY MANAGER AND THE SECURITY ORGANIZATION IN SUPPORT OF MERGERS AND ACQUISITIONS

As alluded to earlier, the importance of security in support of a merger or acquisition can't be overemphasized. All mergers and acquisitions are faced with security issues and concerns. To properly handle them, security managers need to be involved. The extent of security involvement varies depending on the complexity and size of the total effort. Moreover, security issues and concerns vary according to the nature of the business, type of industry, and the maturity of the security programs. For example, security issues common to the banking industry differ from security issues common to the transportation industry.

Security and the security manager plays a supporting role. Like many other supporting organizations, security contributes to the overall success of the effort. Security is not the most critical component of a merger and acquisition team. The merger and acquisition team has a mission to:

- Identify potential targets for acquisition
- Assess those target companies
- Execute the merger or acquisition

The most critical function of any merger or acquisition team is to properly assess the value of a target company. That responsibility lies with the financial team. That is not to say that security is not an important element in preparing for and executing a merger or acquisition; therefore, it should not be ignored or relegated to a role of less significance. The paramount concern of the merger and acquisition team is to identify and properly value a target company.

The financial team focuses on determining the current financial condition of the target company. It also assesses its future earnings capabilities. With that information, a value is placed on the target company. This process is much like the actions of any serious investor when looking for an investment opportunity in any company. Investors seek the optimum deal. A deal that adds value to the acquiring company thus benefits its owners. When one company acquires (purchases) another company, that transaction is an investment. The role of the security manager is to do what is necessary to support the merger or acquisition team in its effort to accomplish this mission.

In any event, security plays an important role on the merger and acquisition team. The security team has a responsibility to mitigate risks and protect the interest of the company, its owners, and shareholders. In support of this obligation, security, as a member of the merger or acquisition team, helps the team make informed decisions and execute a successful transaction.

It is not always apparent to the merger or acquisition team leadership that security needs to be an active member. Nor is it always apparent in the early stages of the effort that the team will encounter situations where expert security support is essential to properly protect the effort and/or its related assets. This is particularly true with new or inexperienced teams.

Team leaders and team members with little to no experience in mergers and acquisitions may not recognize the importance of ensuring that security is an intricate part of the process. If this is the case, it is incumbent on the security manager to work with team leadership and help them understand the role security should play. Doing this early in the effort may help avert security problems from developing later on. Essentially, it may require the security manager to "sell" security to the team. It is important to sell security to team leadership based on real issues and the value security brings to the effort. Don't oversell with exaggerated claims of what security can or should accomplish. Be realistic. The credibility of the security manager and organization is at stake.

Selling security may be as simple as meeting with the team leadership, or all its members, and providing advice and counsel on relevant security issues and concerns along with creating an understanding of what the security organization can do to support the effort. In some instances, selling security may not be so easy and may require the development of a more formal business case characterizing to team leadership the precise value security brings to the effort. In developing the business case, the security professional should keep separate the protective role from the assessment role; thereby ensuring both are communicated and understood.

Team Consultant

Part of the role for security is to serve as the team's "in-house consultant," that is to say, serve as a subject matter expert and help the team learn as much as possible about the target company, particularly as it pertains to matters of security. There are many ways to learn about a target company. If the company is publicly held, much information may be obtained directly from the company itself through its investor relations organization. Moreover, in the United States, information can be obtained from the Securities Exchange Commission, stock market agencies, various publications, and many other sources. Learning and collecting information beyond what is available from these sources requires further investigative work. The gathering of competitive intelligence is a complex task the security manager can and should support.

Other Roles of the Security Manager

The role of consultant to the merger or acquisition team is only one of the important tasks of the security manager. The role of security is multifaceted and the security manager supports the effort in many ways.

Cost/Budgeting

Budgets and expenses must be managed. Every function is responsible for managing its department budget and its expenditures. Security is no exception. The security manager must plan for and manage the cost of security in support of the overall merger and acquisition effort. Additionally, the expected costs associated with providing security to the new company during the postacquisition period must be identified. The security manager must evaluate what resources will be needed to provide security to the company after the two companies merge.

During the premerger period most of the costs encountered by security are labor costs. To ensure that sufficient security expertise is supporting the merger and acquisition team, the security manager uses company security professionals or security consultants to do the necessary work.

During the postmerger period, the security manager focuses on what it costs to provide security to the new company. When two companies come together as one, the security statement of work must be changed. It must be adapted to meet the security needs of the combined companies. With a change in the security statement of work will come a change in the cost of security.

When it comes to spending money on security, one condition is certain: The cost of security for the new company will be expected (by company leadership) to amount to something less than the combined cost of security for the two companies when they were separate. The security manager will be expected to achieve cost savings when bringing two security organizations together. Company leadership will expect the security manager to find opportunities for the elimination of waste and redundancies and to capitalize on any and all potential synergies. Essentially, when it comes to combining two companies or two functions, management has an expectation that one plus one should not equal two. It should equal something less than two. It should never equal more than two.

The security manager must also remember the following:

- Some people will undoubtedly lose their jobs as part of an acquisition or merger and elimination of redundant processes and tasks. Telling people that they no longer have a job is not an enjoyable task. However, it must be done professionally and the sooner the better to eliminate the increased stress and loss of productivity suffered as a result of the merger or acquisition.
- Do not get talked into doing additional work without an increase in budget or a specific budget from which to draw funds to support the merger or acquisition. You will find that other managers will have additional budget available. Don't play the "dedicated, loyal company fool" by trying to do the additional work without additional budget.

Assess Impact to Other Organizations

Security cannot operate in a vacuum. Any analysis of security issues and concerns must consider the impact on the total effort, other functions, and the company as a whole. When assessing security issues, keep in mind the potential impact to affected organizations. For example, if a target company conducts business internationally with operations in high-risk countries, those operations should have in place contingency plans appropriately developed to mitigate those risks. If they do not have contingency plans in place, they may be operating at a higher degree of risk than is acceptable to the company. The extent of that risk varies depending on the size and value of the operation. The team, when made aware of these risks, must acknowledge them and either accept them or mitigate them. In addition, accepting the risks may lead to lowering the value assessment of the target company. Mitigating the risks may cause additional costs. Some organizations may be affected, as they may have to spend money later on to mitigate identified risk. They should know this as early as possible. Depending on the degree of risks and the cost of mitigation, the deal itself may be affected.

Communications

For security, communications is divided into three major categories:

- *Team communications:* Within the merger and acquisition team, communications are generally of a confidential nature. Information related to the merger or acquisition is communicated between team members and must stay within the confines of the team. None of this information is shared outside the team. It is the role of the security manager to define the parameters and requirements for protecting team communications. Clear communication guidelines and procedures must be established and shared with all team members.
- *Communications to employees of the target company:* As the merger and acquisition process evolves, it may be necessary for security to communicate information to employees of the target company or to all company employees. For example, if a change in a security procedure is necessary, that change must be communicated to all employees. A process should be established for all formal communications to ensure that all employees receive the necessary information in a timely manner. Since communications are very sensitive during a merger or acquisition, any communications processes developed must be coordinated with the team and especially the individual assigned responsibility for merger or

acquisition employee/company communications. Conflicting or improper communications must be avoided, as they are difficult to recover from. Because of the sensitive nature of a merger or acquisition, all outside communications should be through the communications focal point. This point cannot be stressed too heavily. Even if approval is granted for the security manager to communicate outside the team on such matters, this communication must be carefully evaluated by the security manager, as any adverse impact caused by such communication will be blamed on the security manager whether or not the blame is valid.

- *Communications within the security community:* Security management must effectively communicate with all members of the security team. These communications should occur regularly and be as thorough as possible. Within this context security communications take two forms: (1) communicating security-related issues and actions to security employees to ensure that everyone is working toward the same plan and the same objectives and (2) communicating to the security team in their capacity as a company employee.

Security professionals and staff are employees, too. Security management must communicate to security employees to keep them as informed as practical concerning the changes occurring within the company. Security employees, like all other employees, experience high levels of anxiety during periods of uncertainty. To keep this anxiety at a minimum, regular and frequent communications are essential.

Ethics

Behaving ethically should not be something employees and management have to be reminded to do; however, this is often the case. Newspapers and business journals are filled with stories of companies and their employees engaging in unethical behavior. Unethical behavior almost always has negative ramifications and will end up costing any company more than the perceived gain. During a merger and acquisition effort, much trust is placed on the merger and acquisition team. Sensitive information, plans, and strategies are shared with team members. Team information is often confidential and requires proper handling and use. In some cases, the handling of information is governed by legal or regulatory requirements. Using any of this information in a manner not sanctioned by the team or company is inappropriate. Misuse in terms of government regulation or law may be punishable with criminal sanctions (e.g., you may be fined and also go to prison!).

Security personnel have the same obligations as all team members—to behave ethically. Furthermore, security personnel are often entrusted with sensitive information beyond that of the average team member. As protectors of information, security professionals should perform their duties to the highest standard of behavior, setting an example for all.

Planning

In any business endeavor, planning is essential. Planning allows a team to think through the activity and identify actions and issues. As actions and issues are identified, they can be carefully considered for alternative actions and implementation. The process of planning causes a team to consider all aspects of the endeavor, good and bad. The process of planning brings the team to a common level of understanding as to what must be accomplished and how it is to be accomplished. The product of planning is the creation of a written plan. The plan itself is the documented result of planning and the metrics by which goals and objectives are measured against. It can be argued that the true value of the plan is the process of planning. For the plan to be most effective, it must be communicated to the team, shared by the team, and, perhaps most important, agreed to by all team members.

An experienced merger or acquisition team will have a plan. That plan should cover everything from the process of identifying target companies to closing the deal and all actions that lie between. A portion of the total plan should be dedicated to security. As a subset of the total effort, a security plan must be developed. The security plan should address security actions and issues for all phases of the effort as a subplan of the overall merger or acquisition plan. The security plan should also include the actions and procedures needed to keep the effort confidential, an operational security (OPSEC) plan. The security plan is obviously most useful when communicated and made available to all of the team members.

SECURITY SUPPORT: PREMERGER AND POSTMERGER OR ACQUISITION

A merger or acquisition can be divided into two major phases: premerger and postmerger. Each phase is made up of different activities and therefore requires different types of support. In the early stages, the security organization should focus on protecting the effort and the team and participating as a team member in assessing the condition of the target company. After the merger or acquisition, the role of security changes. With the initial phase of the effort complete, security shifts to focusing on the protection requirements for the new company. The security manager is also responsible for supporting the integration of the newly acquired business into the existing company. Like every other functional lead, the security manager is responsible for integrating the two security organizations together to form a new security organization. If the acquired company is a large business, integrating them into the acquiring company is no small task. The larger the company, the more complicated and involved the integration effort.

Premerger or Acquisition

During the premerger or acquisition phase, the role of security is primarily fact-finding and protective:

- *Preliminary background investigations:* Learn as much as possible about the target company and its leadership. All knowledge gained early will have value in later phases. The more the merger and acquisition team can learn about the target company the greater the possibility of good business decisions being made.

> ***Due diligence:*** *Such a measure of prudence, activity or assiduity, as is properly to be expected from, and ordinarily exercised by, a reasonable and prudent man under the circumstances; not measured by any absolute standard but depending on the relative facts of the special case . . .*[6]

- *Due diligence:* During the due diligence phase of the effort, the merger and acquisition team has an opportunity and an obligation to take a more in-depth look at the target company. This examination is still limited. How extensive it becomes may require an agreement by both companies. Nevertheless, it will be an opportunity to learn more about the target company than is available from open sources. The time frame for the due diligence is limited but should be sufficient to allow for obtaining enough information about the company so that when this information is combined with data gathered from other sources as well as open sources, chances of making the correct decisions are enhanced. It is during this phase that the team leadership identifies and considers all problems and concerns. The problems are evaluated and a decision is made to proceed with the merger or acquisition or abort the effort.
- *Operations security:* Operations, or operational security (OPSEC), refers to the measures and controls applied to the effort to ensure that the day-to-day activities of the team are protected to the extent appropriate. The security manager is responsible for leading this

[6] *Black's Law Dictionary*, DeLuxe Fourth Edition, 1974.

effort and for developing and implementing the necessary protective measures. Protective measures vary with each phase of the effort, as each phase differs in its need for control. For example, the initial discussion concerning the team's intentions to acquire a target company and the background assessments of that company and its executives generally need to occur under very tight controls. Preventing knowledge of the discussions from becoming public could have competitive and legal implications. For example, if publicly traded companies are involved, information suggesting the possibility of a merger or acquisition could have an impact on the stock price of one or both companies. Consider when Comcast announced its intentions to acquire Disney. The stock price of both companies was immediately affected, with Comcast stock dropping and Disney stock rising. Moreover, much of the information pertaining to proposed mergers and acquisitions is subject to control by government regulations, so companies are obligated to control the release of information.

Day One of the Merger or Acquisition

Actions taken before a merger or acquisition, as already mentioned, are limited for many reasons. Until the acquisition is complete, the acquiring company does not own the target company and therefore does not have the authority or right to do anything that will change or alter the target company. Once the target company is acquired, however, the new owner has complete authority to fully examine all aspects of the acquired company and make whatever changes are necessary. What does this mean to the security manager and the security organization? The security manager is now free to fully examine and assess the security program of the newly acquired company and begin to address issues and make changes. Having been part of the due diligence assessment, the security manager should already have a basic understanding of the acquired company's security program and a good idea of any security problems that exist. Moving forward from this baseline of knowledge, a more detailed assessment should be planned.

Postmerger or Acquisition

In the postacquisition period, the premerger and acquisition work would have been accomplished, including the preliminary background assessment. Furthermore, the due diligence phase can now be expanded into a complete analysis of the security condition of the newly acquired company. Since during the premerger phase there are limits on the amount of information available for analysis, the total assessment cannot be completed until after the merger or acquisition occurs. It is during the post-merger or acquisition period when all data are made available.

The expanded assessment should include a complete threat and vulnerability analysis. Keep in mind that the expanded assessment must be accomplished on the acquired company as it operated in its pre-merger or acquisition environment. Understanding how the acquired company functioned before the merger will be useful when leading the acquired company through the integration phase in becoming part of the new company. Will the security issues of the acquired company impact the new company? If so, how and what needs to be done to mitigate those issues?

Once the postmerger period begins, most of the effort will shift from assessment to integration. Integrating the two companies together requires an integration of the two security organizations. The integration effort is always the most problematic phase of any merger or acquisition. It is often neglected and poorly planned. From the beginning, so much attention is focused on making the merger or acquisition happen and closing the deal—what some refer to as the "sexy part of the effort." The postmerger integration is much less "sexy" and takes much longer to accomplish. A successful integration requires a well-defined end state, as well as a clear and communicated plan to get there.

Changing the Culture of the Organization

In an ideal state, when two organizations merge, a new and desired culture is developed. A desired culture should reflect the values and expectations of the new organization's leadership. This does not happen on its own. Changing an organization's culture requires much work with clear and concise communications expectations. If left unattended, a new culture will develop but it will not be the desired culture. It is possible that the culture of each of the two separate companies will continue to exist in conflict if they are not driven to change. The result will be a dysfunctional condition, with clashes in cultural behavior inhibiting the development of a new efficient and effective organization—the opposite of what the company leadership and owners need and expect.

To achieve a desired culture, the expectations and values of the new company must be communicated clearly, consistently, and often. Behavior that is consistent with the stated expectations and values of the newly formed company must be rewarded. This is as true for the individual functions that make up the entire company as it is for the company as a whole.

Within the security organization, the security manager has the responsibility to bring the two organizations together working toward a common purpose of achieving stated expectations. The security manager must ensure that this is accomplished in a manner that is consistent with the stated values of the company. This is no easy task and achieving success requires the use of integration tools such as the following:

- *Security council:* Establishing a security council can be an effective tool in large companies with large security organizations. A security council is really nothing more than a forum to bring together those charged with implementing and managing the company security program to ensure they work toward a common approach. In essence, it is a forum for the organization's security leadership to come together and work toward the same objectives. A security council gives all of security management a seat at the table. It is a tool of inclusiveness. When two companies come together, each of the similar functions will operate somewhat alike but possibly not the same. Expectations and objectives will differ as each entity holds on to what it knows and what it values. Merging into a single entity will require changing what each knows, the values, and the expectations. Accomplishing this integration will not occur naturally. It has to be designed to happen. Each organization must understand and "buy-in" to a single common vision and set of expectations. Getting there will require developing trusting relationships within a framework of common expectations and using common tools, including common processes and the institution of common policies and procedures. Reinforcing this behavior should be the implementation of common measures and rewards. A security council should be a chartered body established for the primary purpose of being the deliberative body for security's functional issues when the function is large and disparate. The membership should include the organization's senior functional (security) management along with members from other disciplines with a major stake in the security program. This council can also be used as a forum to develop strategies and processes to ensure that commonality is achieved and redundancies are eliminated.
- *Policy and procedures:* Long- and short-term policy changes (not intended to cover every area, but at least the critical areas) serve as an interim operating guidance until long-term objectives are defined. Policies and procedures are considered the company-created rules. They are a declaration of how the business intends to operate. They define the operational parameters. Every company must have a set of company security policies and procedures. They establish the rules within which everyone, including security professionals, are expected to operate. When properly designed, they are a very powerful tool for influencing performance and behavior.
- *Service agreements:* These agreements establish boundaries for continuation of services until more permanent measures can be

taken. They are particularly useful when only a business unit of a company and not an entire company is acquired. They are also useful during a divestiture when a portion of a company is sold but not the entire company. For many reasons, it may be necessary for the divested business unit to remain linked to the divesting parent until provisions can be made for a complete separation. For example, if a divested business unit shares a facility with elements of the divesting company, it may be necessary for the acquiring company to lease back facility space from the seller to keep the newly acquired business unit operational. It may also be necessary for a period of time for the acquiring company to buy back services until the separation is complete. These services may include security services. When service agreements are established they should meet the following conditions:

1. They must be established for a short period of time. As short as possible is best. Continuing the relationship for any length of time will be problematic. Keeping it as short as possible will reduce the likelihood of problems.
2. The type of service provided must be well defined. Leave no ambiguity in the agreement.
3. Service agreements must be part of the sale contract.
4. All security issues must be clearly stated to prevent failures or misunderstandings from occurring in the future.

Service agreements may be a necessary tool and can be a useful tool. Because they are part of the delay in separating the business unit from its parent company, they should be used sparingly.

- *Cost of security:* Cost is always an issue. Within most companies, security is a cost center and not a revenue center. Unless the company is in the business of selling security products and services, security does not usually generate revenue. Like other supporting functions, the security organization exists to fulfill a protective and compliance role. Company assets protection, driven by laws, regulations, and the need to mitigate risks, are the reason security organizations are formed. Moreover, to protect their own interest, most companies establish a set of rules (policies and procedures) to provide a protective framework for employees to operate within. This costs money.

When a merger or acquisition occurs, executive management and ownership have an expectation that value will be created with the union of the two companies. One way to increase that value is to reduce costs. Capitalizing on synergies and eliminating redundancies are common means of reducing costs. Every function within the company will be expected to make a contribution. Security is no exception. There are other potential issues of concern:

- *Disgruntled employees:* Every merger or acquisition brings with it at least one disgruntled employee. Of course there is usually more than one but at the very least there will be one. Human nature is such that someone will not be happy with the deal. Even when owners and management are quite pleased with the transaction, recognizing it to be an important and valued-added event, someone will not be happy. Disgruntled employees can be disruptive. At the very least, they can be difficult to work with and thus create a level of tension within the organization that is enough to disrupt the normal work process. When employees are unhappy about a merger or acquisition, they usually don't keep this to themselves. Some passively resist change and are not supportive of the effort to integrate into the new acquiring company. In some cases, disgruntled employees can be very disruptive. Angry employees are not pleasant to be around. Their negative behavior and attitude may create an environment where unresolved conflict develops and even thrives. This is not a condition conducive to good employee morale, teamwork, and sustained high levels of productivity. In extreme cases, disgruntled employees may act out and even attempt to "sabotage" the integration process. Recognizing disgruntled employees and taking preemptive corrective action are the responsibilities of disgruntled employees' immediate management. Dealing with disgruntled employees may also require the assistance of the human resources organization and security. In dealing with a disgruntled employee, the security manager usually does not need to get involved unless employee behavior or actions create a disruptive or hostile work environment. Should an incident of workplace violence occur, the security manager should be immediately engaged as part of a threat assessment team or incident response management process. Disruptive employees and incidents of work place violence must be handled swiftly and decisively.
- *Working and doing business with governments:* Foreign mergers and acquisitions can be more complex than mergers and acquisitions occurring within the same country. Many factors contribute to the complexity of a merger or acquisition. Pursuing a foreign company greatly complicates the transaction. Success requires an ability to work within the legal, political, and cultural structures of the target company's country. Every country has a different set of governing principles for business activity affecting mergers and acquisitions. Within some countries, the laws and regulations are

friendly toward mergers and acquisitions; in other countries, the laws and regulations are so complex and onerous that they make executing mergers or acquisitions nearly impossible. In other countries only specific industries are afforded protection with antimerger and acquisition regulations. Generally, those industries or sectors are considered national assets and provide a economic power or advantage to the host country. Understanding these considerations; as well as the society and culture of the foreign country, is essential in the earliest stages of a merger or acquisition. Knowing about these issues in the early stages of the effort may prevent a major loss of time and money.

- *Classified government work:* Merging with or acquiring a company that does national security (e.g., classified government work) creates another set of issues. Where classified government contracts are involved, strict regulatory and legal requirements drive how those companies must conduct business. If an acquiring company seeks a target company from another country and that company is engaged in classified government contracts from its host country, the acquisition may or may not be permitted. At the very least, if permitted, layers of separation will be necessary, ensuring the national security interests of the host country are protected. In essence a "firewall" must be installed to ensure that the acquiring company is separated from the target company's host country protected information. These controls are complicated but can be accomplished. For example, if a British company chooses to pursue the acquisition of a U.S. company doing classified work for the United States Department of Defense, the British company must obtain approval for the acquisition from the U.S. Department of Defense and other interested government agencies. Once these approvals are obtained, conditions must be established that ensure that classified information from the host country (United States) is protected from unauthorized release and exposure to non-U.S. citizens. This could even require separation and protection of information from the entire British company. In accordance with U.S. Department of Defense regulatory requirements, formal controls and separations must be established to ensure these separations.[7] If the merger or acquisition occurs between two U.S. companies, both involved in classified government programs, the approval process is much easier, as fewer, if any additional controls, are required. The U.S. Government may require an integration plan along with operational waivers allowing the acquired company to

[7] For specific information see U. S. Government regulation promulgated in the *National Industrial Security Program Operating Manual* (DoD 5220.22-M).

continue to operate in its currently approved mode, at least until formal requests for change are submitted to the appropriate government agency.

WHAT SHOULD A SECURITY MANAGER BE ON THE ALERT FOR WHEN FIRST GETTING INVOLVED IN A MERGER OR ACQUISITION EFFORT?

As stated earlier, the security manager is a critical member of the merger and acquisition team, but that may not be recognized or understood by the team leadership. This is often the situation if the team is an inexperienced team. As a security manager, you must expect to spend time with the team leadership to convince them of the value a security manager or team can bring to a merger or acquisition.

All mergers and acquisitions are not the same. The size and nature of the transaction will drive the complexity of the issues. Unless a security manager is highly experienced with mergers and acquisitions, one condition is certain: more time will be spent supporting the effort than was planned. If the security manager is not experienced with mergers or acquisitions and sufficient security expertise is not available within the company, do not hesitate to seek outside support.

Sometimes, things go wrong even with "the best laid plans." Keep Murphy's Law in mind at all times: If something can go wrong, it will. When it does, immediate attention is necessary. Act swiftly to address and solve problems. Not all problems must be solved right away. Some do and must be quickly recognized. Solving them promptly will improve the team's ability to quickly and properly move through the effort in conducting their assessment.

During the premerger and acquisition phase, the team may have limited access to information. The details of the inner workings of the company will not be fully revealed or understood until the postmerger and acquisition period. At that time, the security manager and the entire team should expect that sufficient information will be available to the team to allow them to value the target company and determine if there are any major security issues. Less obviously, issues will not surface early. Usually these issues develop during the postmerger and acquisition period when the integration of the acquired company into the acquiring company occurs.

Remember why companies engage in mergers and acquisitions. They are done for strategic reasons and always with the intent to add value to the acquiring or newly formed company. Much of the newly created value lies in the skills and capabilities of the employees and management team from the newly acquired company. It is a natural reaction for the acquiring company to want to keep the most skilled employees from the acquired company. It will not be a simple process or natural reaction to follow through.

With few exceptions, skilled newly acquired employees will not be kept at the expense of employees from the acquiring company. Not all employees are let go. Most are often retained, as they are needed to perform the work and produce the products that made the company they work for such an attractive acquisition target in the first place. Almost always, some will have to go. Some companies will conduct a competitive bidding process in an attempt to identify the most skilled people from both companies, place them in critical positions, and release those considered to have less value or to be less skilled. Other companies will focus on eliminating redundant jobs and redundant people with little or no consideration of talent.

What does this mean to the security manager or security professional? If you are with the acquired company and are directly supporting a business unit or contract, you are likely to be left in place. Odds are your services will still be needed. If you are a security manager or professional working at the corporate headquarters, start looking for work. One of the first organizations eliminated in any acquisition is the acquired company's corporate headquarters structure. Immediately upon acquisition, a second corporate headquarters becomes a redundant and costly burden. Swift elimination is the cure.

MAKE OR BUY: SHOULD A SECURITY MANAGER OUTSOURCE WORK TO CONSULTANTS OR KEEP ALL WORK IN-HOUSE?

Like every other business function, security is faced with budgetary constraints. Operating within a budget and fielding the most efficient and effective organization is a difficult task. Security departments are staffed with employees possessing the necessary experience and expertise to accomplish the organization's statement of work. They are generally not staffed with reserve resources they can deploy to special assignments as needed. The condition is usually to the contrary. Security departments are staffed at some minimal level without excess resources to divert to efforts as large and important as a merger or acquisition. Furthermore, since mergers and acquisitions occur so infrequently, the likelihood of having employees experienced with them is low. Therefore, when a merger or acquisition occurs, the security manager must make a decision to pursue one of the following courses of action:

- Add to the security staff by recruiting skilled personnel experienced with mergers and acquisitions.
- Allow current staff to take on the challenge of working security issues for the effort, possibly leaving other work to be completed at a later date.
- Hire an outside expert—a consultant—to provide guidance and direction to the security staff to support the effort, or possibly hire the consultant to do the work.

Essentially, a decision to make the service or buy the service must be made. That is to say, provide security support from within the organization using company security professionals or seek the support of external experts and purchase their service. Mergers and acquisitions can be complicated. None are simple; they all vary in size and degree of complexity. All require security support to some degree. If a security manager has never been involved in a merger or acquisition, getting outside help from an experienced consultant is a prudent course of action.

If Assistance Is Needed, Get It

If a security manager or the security team is not experienced with mergers and acquisitions, it is a good idea to solicit help. Help can be obtained from many sources, including from within the merger and acquisition team or within the company. Team members experienced with mergers and acquisitions are good resources for identifying potential sources for assistance. It is foolish to proceed without capable support regardless of where that support comes from.

An inexperienced merger and acquisition team may not understand the need for outside security assistance, or, because of budgetary constraints, the team may not authorize external support. In this situation, the security manager will have to rely on the best effort of the security team and security professionals. There are low-cost options available to a security manager where support may be obtained. These options may not be the best choice, but they can be useful by offering guidance to help navigate through the merger and acquisition process. The following are potential sources for assistance:

- For premerger support, experts within the company may be a valuable source. During the postmerger period, experts within the acquired company may be useful.
- The security manager's personal network of security experts and colleagues: A security manager can consult colleagues who may have experience with mergers and acquisitions, "picking their brains" and learning from their experiences. Until a merger or acquisition is made known, this should only be done in a limited way never revealing anything about the target company.
- Consult the available literature including journals, articles, and books. There are publications devoted entirely to mergers and acquisitions that may be useful. Large libraries and on-line book sellers are good sources.
- Professional associations are another potentially valuable source for information. The American Society for Industrial Security

maintains a listing of currently available security publications that may be helpful.

- Companies offering security services usually have an experienced investigative capability to include experience with due diligence efforts. Some of the larger security consultant firms and service providers may have a wide range of experience with mergers and acquisitions. There are also law firms with this expertise. They may be expensive but will possess the necessary skills to provide quality support. Their expense must be weighed against their value. After all, "doing it right the first time" with experienced professionals may in the long run be a more effective and efficient way of merging companies together.

One problem of seeking assistance from outside of the company is that it expands the number of people with knowledge of the effort. It also requires releasing sensitive company information to persons not part of the company. This concern can be simply addressed. Support can be obtained without exposing or compromising the confidentiality of the program. Use of trusted sources who sign nondisclosure agreements will greatly reduce the risk of compromising information. A good security practice is to have all team members, including security personnel from within and outside of the company, sign nondisclosure agreements. It serves as a reminder to all participants of the importance of protecting sensitive information. Furthermore, should someone deliberately misuse information, having a signed nondisclosure agreement will assist with any necessary action for recourse.

SUMMARY

Whether it is an acquisition of an entire company (total assets), a product line, or two equal companies merging together to form a stronger and more capable company, there will be a requirement for security support and a role for the security manager. The security effort may be as simple as providing guidance and basic security support to the merger or acquisition team, or it could be as extensive as creating a full-time security team to support the effort.

Recognizing the need for security support is not always the case with merger or acquisition team leaders. A security manager may have to "sell" security to an inexperienced team. Moreover, a security manager may have to go outside the company to obtain necessary expertise if it is not available within the company.