CHAPTER 1

Risk Consultancy and Security Management

Most organizations would not go into business without insurance coverage, yet surprisingly few have systematic and integrated programs to address the issue of business continuity, or have qualified in-house expertise to support risk management and operational delivery. The globalization of commercial risk has led to a greater appreciation of the need for corporate planning to identify and manage a wide spectrum of threats to business success through the use of risk consultancy and security management.

Although no organization can prevent all crises from occurring, everyone can lower the odds of their occurrence while also mitigating the negative effects a particular crisis might have on brand confidence, business and operational productivity, market reputation, employee morale, and corporate liability. The importance of risk consultants and business managers in the field of business continuity—as a means by which to identify, address, and manage crisis events—has grown during recent decades, primarily because both government agencies and commercial businesses have suffered significant losses through inadequate risk analysis and the ineffective management of crisis events. Business continuity (and those security professionals who assist companies in the design and implementation of associated policies and plans) forms the foundation of how any organization prepares for situations that might cause business interruption, thereby jeopardizing the core mission and long-term health and sustainability of a group or enterprise.

Risk consultants and security managers manage the relatively unaddressed and widespread needs of convergence within an organization; they bring together often disparate groups and resources to achieve a unified and holistic risk solution. Given the current global climate, every business, regardless of its nature and geographic footprint, should hire qualified and experienced security professionals to establish comprehensive risk management policies and plans. Such plans allow companies to identify, avoid, manage, and recover from a crisis, sustaining business continuity under the most challenging circumstances.

Companies should also understand that risk consultants and security managers provide more than just security-related services. They can be leveraged as business enablers, allowing businesses to make better-informed decisions before committing finite company resources to a venture, allowing corporate leadership to map risks against potential commercial gains. Security professionals can positively affect all layers of an organization's management, from supporting business managers in developing more competitive business solutions, to enabling project managers to design more efficient and productive project plans prior to investment or risk exposure.

As security professionals play increasingly important and elevated roles within companies and their corporate boardrooms, advising chief executive officers (CEOs) and

executive leadership on their company's risk exposure while concurrently coordinating multidisciplinary solutions, the importance of making risk management an integral element of a broader corporate strategy increases. Companies now better understand that they can choose to avoid, transfer, share, mitigate, or accept risk and that risk and security managers are evolving to bridge the gap between corporate leadership, strategic business units, program managers, and other company divisions.

While many of the benefits derived from risk consultants and security managers overlap, companies should understand that security consultancy and management services are entirely different in nature and scope. Each comes with unique and particular requirements and professional skill sets, both within a contracted security company, as well as among the managers or consultants the company may field. Companies should also understand the nuances of expertise connected to both categories; the selection of qualified management personnel should reflect the specific functions the company expects from them. By understanding the differences associated with each area, as well as how they might be merged to provide a combined service, companies will achieve more productive risk mitigation and security management, and therefore better business and operational results.

Often companies with limited in-house risk consultancy and security management resources seek external support on a case-by-case basis. The provision of successful security services as a whole often depends on a security provider's ability to determine what the company wants as well as what it actually needs; many times companies require professional assistance with determining their security requirements. Both parties should have a clear understanding of consulting and management service expectations, capturing these needs under a contract that sets the parameters of services, both *expected* and *funded*. Although this may seem to be obvious, often companies are unsure of the scope of what is required and will seek more support than is either envisaged or funded during the life of a contract—effectively resulting in *scope creep*. This can present both positive and negative challenges for the security provider, as the company (or clients) becomes reliant on the provider and offers opportunities to further develop the relationship and explore new market opportunities. Conversely it also presents a challenge to contracted vendors, as the company's management may make requests or create requirements for support outside of the contractual and funded agreement. Careful balancing of both factors is necessary to ensure success by both parties and also prevent the company from placing unrealistic expectations on their provider for work that does not result in revenue generation or, worse, results in financial or capability losses.

Fundamentally, consultancy and management are distinctly different services, although both may be required in unison under one contract. Risk or security consultancy is basically the provision of specialist security advice and guidance, whether it is providing security surveys, audits, policies, business recommendations, or procedures, often with an eye for concurrent business development opportunities. Risk or security management is effectively the managerial and administrative control and coordination of personnel and assets, providing advice and guidance in terms of how best to manage project operations, with a smaller degree of attention to business opportunity, as shown in Exhibit 1.1. These two services can be provided concurrently as a unified service, where the specialist supplies advice to establish the need and approach, then services or directs the resulting tasks.

The distinction between the two services, consultant[1] and manager, is, however, often unclear to a company, which may envision a combination of the two functions supporting their task when actually contracting for only one service. Both the company and the service

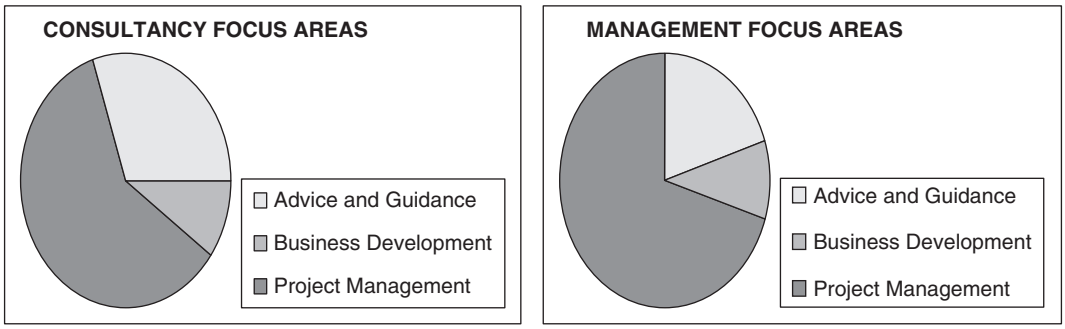

Exhibit 1.1 Risk Consultancy and Security Management Focus Areas

provider must clarify and articulate the difference. Likewise, where a combination of both elements is required, and as the project grows in needs, both company management and the security provider should seek modifications to a contract to support the provision of unforeseen services. This is important to both parties, in terms both of staying within the parameters of the contract and in avoiding problems associated with providing services that could come with legal or reputational issues, or result in the provider breaching the contract's service deliverable terms by focusing on the wrong task areas.

It is also easy for local vendor management to slip into a habit of providing more and more assistance, to the point where they are supplying a considerable amount of additional unpaid effort. This is more so the case for security managers, where they are asked to contribute to policies, plans, and strategies rather than focusing on running the security resources. For vendors and companies alike, this can be considered good business practice up until a point, but in some cases it can negatively affect both the company and the provider if a sensible balance is not struck. While clear distinctions and agreements should be made with regard to the funded services being contracted for, it is worthwhile to remember that it is often useful to provide *additional* services in the short term (until a contract modification can be made) in order to retain a healthy intercompany relationship. The service provider should seek to achieve the balance of helpfulness and pragmatism, without being taken advantage of or alienating the company's management, and the company should seek to compensate the service provider to acknowledge the additional and often unfunded efforts undertaken.

The distinct differences between consultancy services and program security management are discussed in greater detail in the chapters that follow. This chapter is designed to set the scene regarding how security services, both consulting and management, operate between company and service provider or vendor organizations.

PROJECT PLANNING

Ideally the company will engage a security provider or individual consultant at the beginning of the business activity's life cycle, prior to any actual work being started. Consultants therefore are best placed to gain a better understanding of the project requirements and dynamics before any plans are made and resources are allocated by the project team. This allows

consultants to influence the strategic planning of the company from the outset, preferably in alignment and partnership with the business team targeting a specific opportunity. Consultants arriving midway in the business or project life cycle will face additional challenges; concepts and plans will have been developed independently of advice, and budgets and funding may have been set. As a result, it will be psychologically harder, and probably more costly, to modify such concepts and plans as resources may have already been contracted and mobilized, and changes may interfere with an activity or incur unaccounted-for costs. In the ideal situation, consultancy or management services will be provided before plans are made and resources mobilized, ensuring that the company's and the project's plans are developed and aligned with actual needs, saving time, money, and effort in the long run.

It is important for the consultant to understand the dynamics that affect different individuals within the company and project organization, not just in terms of the roles and responsibilities, but also regarding the organizational peculiarities, structures, human dynamics, and office politics residing in any group of professionals. By understanding the goals, objectives, and concerns of different company managers, the consultant will be better positioned to offer observations and recommendations in a manner more likely to gain traction. In addition, the security or risk management element of some companies might have an equal voice within the overall management structure, while in others they are relegated as an afterthought and might even fall under the health and safety officer or in the human resources department.

While security providers and their consultants may interface with multiple parties within a company, from the CEO to legal, contracts, and projects, typically there are three practical interfaces the consultant will deal with to complete the actual task itself:

1. *Business manager*. Business managers are responsible for targeting opportunities and gaining board approval to enter new markets or expand existing regional business opportunities. Often business managers are motivated by financial targets and have quarterly or annual targets to meet in order to grow client portfolio and business revenues. They lead capture teams in order to present business solutions that meet client quality and cost needs, and often view security as a cost element that might undermine the probability of their success. Business managers who are grounded in risk and security management seek security as a component of their solution, understanding that it will increase the value of their proposal. Those who are unfamiliar with operating in remote or challenged environments will be less inclined to consider the applicability of risk and security within their approach.
2. *Program/project manager*. Program/project managers normally seek to achieve the milestones set for the activity in terms of objectives, schedule, and cost. Their task is to ensure that the business activity achieves what is expected, when expected, and within budget. Aside from their professional responsibilities, most companies link the career and bonuses (perhaps a percentage of the actual contract value) of program or project managers to achieving these objectives, with every cost and delay to the project reducing the value of the personal incentive award. As such, poor management typically focuses on getting the job done rather than focusing appropriately on risk, while strong managers will seek advice and guidance to identify and manage risk as a proactive project approach. Both company risk managers and security vendors will need to balance the corporate and personal drivers against their own task of mitigating risk and providing

good service. Good managers will balance both project goals and risk consideration; others may view risk and security an unnecessary hindrance.

Security providers or in-house security managers who are able to offer recommendations that directly focus on objectives, schedules, and costs, while concurrently mitigating risks, will better support the company's project success and will more likely gain better traction with executive leadership. Those security providers or in-house security managers who focus on risk mitigation in isolation, and who do not consider the business objectives within every risk decision, will have a limited ability to place their role within the wider context and will not enable the most productive business results.

3. *Security manager*. A company may assign a different name to the management position responsible for managing risk and coordinating security services, or may subsume the role within a more generic corporate position, such as under health and safety, human resources, or the legal department. For those companies operating within more challenging environments, a defined position is often required to directly focus on risk mitigation. Security managers are often in the difficult position of providing observations or recommendations that might be viewed as constraining the productivity and speed of the project as well as incurring unnecessary costs. Typically security is considered a cost center rather than a means by which to conduct productive business or project activities.

   The difficulty is further exacerbated as the security manager is embedded within the company, and thus the manager's career and livelihood may depend on retaining a good relationship with the business leaders as well as the program and/or project manager, rather than offering frank but unpopular recommendations. The security manager will be focused on balancing his or her own company's office and management politics, ensuring that the recommendations do not discredit him- or herself or increase activity costs. The security manager will also seek to ensure that any security vendors are best exploited on the company's behalf, while also that ensuring risk is mitigated and security is provided at an appropriate professional level. The security provider should be aware of these factors in order to best support the security manager, as well as to identify the best approach to achieve the desired risk mitigation and security measures needed to protect the company.

BALANCING SERVICE DELIVERY

While every contract and project has unique needs, the general principles of security consultancy and management remain the same. There are three interconnected areas a company and their security provider must balance when managing a contract:

1. Contract requirements and company expectations.
2. Provider's business needs and service delivery standards.
3. Project and environment risks factors.

The weight of each factor will differ, depending on the company's business goals, expectations, and the corporate risk tolerances associated with both the project and the environment in which the contract operates, shown in Exhibit 1.2. The security provider will also

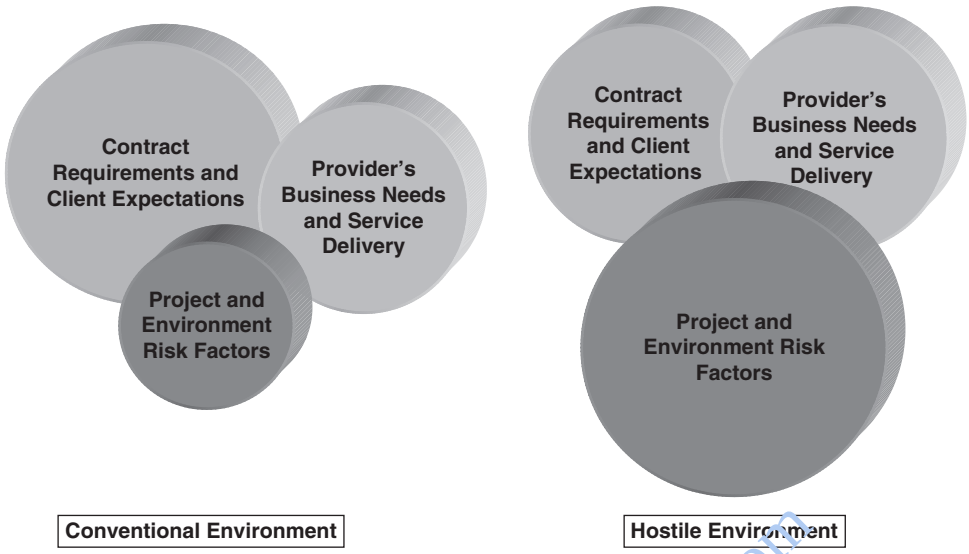

Exhibit 1.2 Balancing Service Delivery in Different Risk Environments

bring its own needs to the task, including its business objectives and corporate risk tolerances. In a conventional or nonhostile project environment, the relative importance of these three areas will vary depending on the contract's specific requirements. A consultancy or security contract in a conventional environment generally will focus more on the company's expectations and the provider company's business needs, with risk mitigation concerns being a smaller area of consideration. Conversely, in a hostile environment, the risk factors and mitigation measures play a more significant part of contract consideration, with company and provider business needs and project interests being proportionally reduced in relation to risk considerations.

Of course, all factors are interconnected and must be viewed holistically, as risk is connected to the company's ability to perform project tasks to standard, on time, and within budget, and effective risk management protects the company from physical, financial, delivery, reputational, and liability risks. It is also important for both the company and the security provider to understand that every action creates a reaction, and that the project activities themselves may increase the risk factors by raising risk profiles or providing opportunities for unwanted attention and thus in turn influencing the contract requirements and subcontracted security provider's business needs, creating a cyclic process of reevaluation and contract change.

Contracted risk consultants or security managers supporting a task will be most effective if they understand the business needs of both the company and the contracted vendor, placing these needs into the context of the varied risks faced by both, from corporate and strategic concerns to the more personal or granular levels. Balancing service delivery requires consultants to be positioned to offer the best advice and service, meeting as many individual and group interests as possible. For example, at the granular level, the consultant and the company's risk manager may wish to identify where a project manager, whose bonus relies on the timely completion of a task, may be more inclined to place him- or herself and others at risk, increasing the focus on contract requirements while reducing the value of input from

the security provider as well as the attention paid to mitigating postulated risks. Often robust service delivery management is necessary to balance business needs against those of risk management.

Alternatively, a company with a low risk threshold that is unfamiliar with a new environment or activity may view the risk mitigation advice and security services provided by a vendor as a means of operating within an environment that it otherwise would avoid, thus increasing the importance of the security provider's input within a contract. Company risk managers should be cognizant of the vendor overtly or covertly imposing its own tolerance levels or risk perceptions to executive management and seek to ensure that the correct balance is achieved.

The table below offers some considerations to indicate how both the company and the security provider's focus on each area of consideration may vary.

Expectations	Impacts	Risk Focus
Company payment tied to schedule	More inclined to take risks to ensure timely project completion	Low
Company payment tied to performance	More inclined to allocate monies to mitigate risks during contract	High
Company has low risk threshold	Likely to withdraw from project if risks increase or injuries occur, or invest in risk mitigation	High
Company accepts high risk threshold	Higher likelihood that risks are accepted; possible cavalier attitude and lower investment in risk mitigation	Low
Company defers security responsibilities to vendors	Company may force definitive provider agreements to achieve project needs and may demand unrealistic or high-risk services from security vendors	Low
Company dependent on security provider/vendor for decision making	Company reliance may result in greater acceptance of advice and guidance, limiting the ability to conduct quality assurance of security vendors	High
Security vendor values its own reputation	Security vendor may refuse work, or take a strong position on accepting risk in order to protect its reputation or liability exposure	Varies
Security vendor's business development goals important	Security vendor may accept higher-than-normal risks in order to grow business quickly	Low
Security vendor has low liability tolerances	Greater focus on liability risks, especially injuries and deaths, thus driving more candid and realistic recommendations and approaches	High
Security vendor's experience in service	Experience varies the balance of company/risk/business needs	Varies

(continued)

Expectations	Impacts	Risk Focus
Risks posed direct to project	Threats posed directly to a project result in greater focus on risk through specific project-targeting threats	High
General risks high for region	General risks may result in more balance between project needs and risk levels	Medium
Project faces low risks	Low risk levels may result on a greater focus on the business needs	Low
Only provider faces risks	Providers who face all risks focus on their own business needs; companies may accept higher risk levels as they will not be affected	Varies

The company effectively has the final vote on what level of security is provided, as it controls the budget and may change security providers who do not meet its requirements or expectations. That said, sound company management will consider the advice and guidance offered by security professionals, both internal and external, in order to strike the correct balance between business needs and risk management. Good security vendors will offer candid advice in order to provide the best service. However, human dynamics play a significant role in how effectively management decisions are made. Often the balance is not achieved and risks outside of corporate tolerance levels are accepted at a local level.

COMPANY AND VENDOR RELATIONSHIPS

The development of a strong professional relationship between the contracting company and the security provider's management often underpins the levels of success of the business venture, as well as the ability to provide productive consulting and management services. Disjointed management relationships, groups operating in isolation, or the failure to understand the business needs or to acknowledge risk factors will place all personnel and companies at avoidable risk. As with any management structure and process, integration is vital, especially within hostile, remote, or new business environments.

It is also important that the company and security provider management and personnel understand that often the contracted company cannot force an issue, only advise and manage risk. Thus if project management or staff choose to ignore advice and guidance, often the risk consultant or security manager is authorized only to raise and document concerns, rather than physically force the correct measures to be implemented. In the most extreme cases, security providers can refuse to conduct a task or undertake an activity; however, they still have limited control over the activities undertaken by their clients independent of their support. Clear parameters of authority and responsibility need to be established between the company and vendor so as to address, effectively and clinically, areas where professional disagreements may present risks to personnel and activities. The sections that follow offer real examples of cases where company management has been both dismissive and receptive to their security consultant's advice.

Client Meeting

The security consultant operating within a high-risk environment advised the project manager that the meeting should be held at an alternative venue due to high physical risk levels at the proposed venue. The project manager insisted that the meeting go ahead as planned. The consultant then offered documented mitigation measures to protect the manager's plan, citing the use of armored vehicles during movement within the venue area, the conduct of discussions within hardened buildings, and the need to stay at a defined distance from the perimeter boundary. The project manager subsequently ignored most of the advice during the visit. During the manager's visit, a mortar attack resulted in an unexploded mortar round becoming lodged within the engine of the soft-skinned vehicle used for the manager's movement. (The project group was standing 80 feet from the vehicle when it was struck.) Two soldiers were also injured by snipers on the perimeter fence. The consultant had documented each assessment and recommendation for clarity and audit, thus fulfilling his and his provider company's obligations to provide risk mitigation services. It was not within his authority to prevent the visit, only advise on the risks and mitigation measures associated with each task component.

Project Planning

The security consultant provided detailed risk mitigation measures required for the development of a project site located within a remote and hostile area. The security footprint involved the use of local police and military personnel to provide an outer security layer, with a secured and hardened compound to permit construction activities to occur within a relatively protected space. The consultant advised against frequent site visits due to the high incidence of attacks along the limited routes to the project site. The project manager opted for frequent site visits, with the project remotely managed using entirely local contractors. It was recorded (prior to the manager's decision) that each day a visit was conducted, an improvised explosive devise (IED) had been placed on one of the routes used (although not directed specifically at the visit team). Several weeks after the assessment, a complex attack was mounted specifically at the project team. The project closed prior to completion, resulting in approximately $50 million of failed project costs to the funding government.

Threat Prediction

The security consultant advised the program risk manager that intelligence resources had reported a serious surface-to-air threat within the local region as well as specific targeting details. The consultant advised that air movement be delayed and countermeasure equipment be installed within the company charter aircraft. The program manager, noting the agreement reached between the company and security vendor risk managers, authorized aircraft to be grounded for 20 days until the postulated threat had diminished and invested in counter surface-to-air equipment. These actions resulted in significant costs and disrupted operations, however significantly reduced risks to the company and employees.

Misinformation

A specific project manager was known to be discussing large-scale personnel movements and project plans with a wide local audience, placing himself, his project staff, and the security team at significant risk. He provided verbal and written details on the dates and times a project location would be demobilized, offering an ideal opportunity for insurgent targeting. The provider consultant advised the company risk manager and program manager of the unnecessary and avoidable risks being created through poor information security, advising that misinformation relating to demobilizations be provided to the project manager and all project staff. The program manager agreed, and false dates and times were provided to his subordinate, which were duly passed to the same wide audience. The extraction of the project location then occurred early morning, 24 hours prior to the false extraction date, with no resulting incidences.

CONSULTANTS' OBJECTIVES

It is important that both the company and the security provider's management understand the objectives and responsibilities of their consultants. Consultants will have three main objectives during their appointment:

1. To look after the interests of the company they work for (the vendor).
2. To provide the best level of service to support a contracting company's project.
3. To ensure that they maintain their moral obligation to ensure the safety of those individuals they are responsible for. (This aspect becomes particularly important in challenging environments.)

The next lists capture some key areas consultants should consider when providing services to a contracting company on behalf of their employer.

Interests of the Provider Company

- Provide services that best reflect the standards of the provider company.
- Identify reputational, liability, and contractual risks to the provider company.
- Provide services meeting (or exceeding) contractual requirements and/or company expectations.
- Ensure further company requirements are identified and raised to the appropriate vendor management personnel, then contractually bound.
- Ensure invoicing is accurate and timely and that problems are identified and resolved.
- Ensure further business opportunities are identified and raised with the appropriate persons.
- Ensure all documentation is produced to the highest of standards.
- Ensure that internal and external auditing requirements are identified and addressed.
- Ensure quality control over all subordinate security management.
- Ensure that safety and security are central to all operations in remote, challenging, new, or hostile environments.
- Ensure a strong company relationship is maintained at all times, exploring new business opportunities.

- Report all pertinent matters to the appropriate management in a timely and detailed manner.
- Ensure all materials, assets, and equipment are accounted for.
- Keep clear documented records of significant project matters, problems, and incidents.
- Quantify and evidence all recommendations where possible.

Interests of the Contracting Company

- Understand the technical nature of the project, its schedules, incentives, terms, and conditions.
- Understand project risks, problems, and impediments.
- Understand the risk tolerance levels of the company as well as the program/project manager.
- Proactively identify possible project delay factors, with recommendations for mitigation.
- Provide succinct and accurate verbal and written materials to support project operations.
- Establish methods in which the company might succeed rather than offering negative solutions. Also offer varied options.
- Assist company management in their business goals, working as a partner where possible.
- Be able to work with limited information and evolve plans in alignment with changing needs.
- Identify provider company shortfalls and resolve them before the company becomes aware of them.
- Offer (permitted) additional support, in order to grow further business.

Interests of the Contracted Staff

- Refuse where necessary (last resort) to sanction activities that exceed risk security provider company's risk tolerance levels.
- Clearly articulate and document risks faced to personnel; address them with mitigation measures.
- Seek written direction for unwarranted risk acceptance by the company or security provider company.

CONSULTANT SKILL AREAS

A number of factors define the skill sets required of a consultant: the nature of the service being provided, the type of company being serviced, the environment in which the project is operating, the cost allowances, and so on. Each consultancy role may have particular needs that define the unique requirements of each service or task. The next list details some of the generic skills often found in successful consultants.

- The ability to identify and foster further commercial opportunities.
- The ability to balance the operational requirements with a sound commercial awareness.

- A solid foundation of knowledge and experience within the service to be provided to the company or client.
- The ability to quickly grasp new concepts and industry areas to enable the provision of more tailored solutions.
- The ability to inspire confidence and trust within a company, notably in hostile environments; an authoritative and credible manner when speaking on relevant subjects.
- The ability to communicate clearly and concisely with the company, both verbally and in writing.
- The ability to take a contract from inception, through the proposal stage, into contractual terms, and then run the contract in terms of delivery, expansion, invoicing, and standards, handing off to security managers.
- The ability to understand all forms of risk, to the company, the vendor, and contracted personnel.
- The ability to establish information and relationship networks to support both company and vendor interests.
- The capability to relate to the company on both personal and professional levels.
- A balanced and levelheaded demeanor under trying conditions.
- A clinical and focused approach with a keen eye for detail.
- The ability to view complex security issues holistically, placing them into a project context.
- Strong management skills, fostering good team spirit under challenging conditions.
- The aptitude to deal with crisis situations with confidence and professionalism.
- The ability to quickly adapt to new requirements and changes, in both risk and project terms.
- Good information technology skills, allowing for the presentation of information in an understandable and professional format.
- A proactive and imaginative manner in approaching contracts and in developing new systems and policies to enhance service delivery.
- The ability to research and analyze information quickly and effectively.
- The ability to view operational requirements from a commercial perspective.
- The ability to identify resources that may be leveraged to support the company at no or low cost, especially governmental agencies.
- The ability to establish external relationships that bring value to a project or contract.
- The ability to see cross-utilizations to best use limited or finite resources.
- The ability to think at both a strategic and tactical level, bringing innovation as well as common sense to bear.
- The ability to design policies and plans that lend themselves to efficient adaptation and adjustment.
- The ability to balance tact and diplomacy with honesty and candor.

PRINCIPAL CONSULTANT ERRORS

The field of *security services* encompasses a number of industry sectors, from the more management-oriented services such as risk consulting, investigations, due diligence, project operations, cybersecurity, intelligence, and business facilitation to the harder edge and more

practical services such as close protection, cash in transit, critical infrastructure, and event protection. Although service leaders generally have a solid grounding in many of the principles of risk and security management, many have little transitional awareness between government to commercial appointments or an appreciation for the unique principles of commercial application. Government-sector risk tolerances and perceptions are also very different from those in the commercial sector, and many companies are exposed to unnecessary risks by failing to structure or define their contingency and crisis management approach. In the past, too few companies required, supported, or provided education and standards for those responsible for developing risk management policies and implementing security procedures within the corporation.

Today's well-grounded security professionals understand the principles of convergence, helping their company bring together multifaceted resources to leverage organic and external capabilities, reducing operating costs, and increasing overall organizational performance. Commercially attuned security professionals also understand the tenets of business continuity; they are able to identify and avoid risks as well as develop policies and plans that allow an operation to function during a crisis or to recover following a catastrophic event. To be successful in this evolving and maturing field, security professionals must also understand the holistic nature of risk and how both tangible and intangible risk impacts can result in ripple effects that move through an organization. Security professionals are increasingly integrated as part of business and project teams, supporting both business leaders in developing an environment in which a pursuit may occur and program design within a risk context. Increasingly security professionals are becoming facilitators for business success, important cornerstones for corporate planning and decision making.

Consultants entering into a contract may have a background within the commercial sector they operate in or may have recently left military, law enforcement, intelligence, or other specialist organizations. Those consultants new to a particular field may inadvertently place themselves, their client, and their parent company at risk. While those entering the commercial consultancy or management fields from these backgrounds may on the surface have a solid foundation of experience and capability that might support their newfound civilian careers, the transition between government and commercial operations is often surprisingly difficult, even for the most senior-level managers.

Typically the management risks posed to a company do not take the form of physical threats, as those with the relevant backgrounds within security naturally identify and mitigate against these more obvious and tangible threats. However, noninstinctive risks, such as contractual requirements, invoicing, legal issues, policies, and reputation, tend to be errors common among new consultants. Many lessons are learned the hard way with consultants assuming knowledge in areas for which they have no real expertise, or by being overly eager to help a company in a manner that later compromises the provider company's ability to compete for future contracts. These errors include:

- Jeopardizing the security vendor's contract.
- Undermining the vendor's professional standards and reputation.
- Placing the vendor and its employees/subcontractors at liability for professional or personnel misconduct.
- Preventing the vendor from billing/invoicing the client effectively.

- Preventing the vendor from demonstrating that proper operational procedures were carried out.
- Preventing the vendor from demonstrating that policies and procedures were adhered to for audit purposes.
- Undermining the safety and security of company and vendor's company personnel.

The next list illustrates some of the most common and serious errors within the consultancy and management field that can affect both the company and security vendor.

- *Providing inappropriate documentation to a client*. In an attempt to assist clients in their proposal-writing tasks, consultants have often unwittingly excluded the vendor from competing for certain contracts. This occurs principally in government contracts when a consultant provides written inputs that a client later uses within a formal statement of work, which is then included within a scope of work for a government contract for which numerous bidders offer proposals. The vendor may then be legally excluded from competing as it violates government conflict-of-interest regulations, resulting in loss of considerable potential revenue. (See Chapter 13.)
- *Treating the client as a friend*. Living in close proximity with clients for protracted periods of time, often under difficult conditions, can naturally result in the formation of strong personal relations between the consultant and company management. When the fine balance between establishing a strong relationship and being inappropriately friendly is crossed, consultants may offer inappropriate personal opinions, thoughts, or advice to company staff. Management personnel may also use consultants as tools by which to achieve personal goals, thereby jeopardizing the contract and contractor as well as damaging a vendor's reputation.
- *Using incorrect pricing for services*. Consultants may offer the company a price for a service or assets without clearing it through the appropriate contracts, finance, operations, or other appropriate managers. The product or service offered then may be found to cost more than the stated amount. The vendor may have to change the price offered, damaging the provider/company relationship; worse, it may not be able to bill for the correct amount, thus incurring considerable financial losses. This is not in the interests of either party as it creates uncertainty and impacts both business groups.
- *Discussing wage rates or actual costs with clients*. Vendor consultants may not fully understand the hidden costs of sourcing, procuring, and managing labor and equipment, thereby passing incorrect and proprietary information to client company management. This places the vendor at a competitive disadvantage if the company uses information as leverage against the vendor, assuming the vendor has lower overhead costs than it actually has. Secondarily, it may cause the company to doubt the consultant's ability to guard sensitive information that it may not wish have exposed to a third party.
- *Speaking of specialized areas without the relevant experience*. Consultants may offer information based on limited or out-of-date knowledge regarding a specialty or technical area. The project team may take this as specialist advice as truth and plan their project requirements accordingly, leading to the implementation of poor operational or contractual plans that might threaten company personnel and incur reputational or liability risks to the vendor.

- *Assuming knowledge of regulations*. Consultants might make unilateral decisions regarding contract provisions based on a faulty assumption that they possess sufficient knowledge of corporate, government, or legal regulations. This could result in significant financial losses to the vendor as a result of failing to follow these regulations; notably it may prevent accurate and timely billing for services rendered.
- *Offering services without contractually binding documents*. Often project management request services that have not been formally or contractually authorized. Only recognized authorities within the company's corporate structure have the authority to commit funds and this authority may in fact not rest with the management element requesting services. There are contractually recognized means of communicating these requests, and consultants must ensure they are used and present before rendering services. Verbal agreements, e-mails, or requests from unauthorized project management personnel may not be sufficient to justify later invoicing for services—although with well-established relationships, these may be sufficient. If proper and binding policies are not enforced, the billing for services may be denied, leading to considerable financial loss and project disruptions.
- *Auditable operational planning documents*. Consultants may not document operational activities properly. Proper documentation can later be used to demonstrate that the correct intelligence and risk mitigation was conducted and that operational planning was professionally implemented. During an audit, or after a serious incident, a lack of documented proof that appropriate planning measures were in place for a task or project may place individuals and both the company and the vendor at liability or reputational risk.
- *Not retaining detailed and well-structured databases*. The consultant's hard-drive information may be owned by the company or funding government and may be subject to audit several years after a contract has been completed. Also, when a contract closes, consultants invariably are difficult to locate or use to assist external parties in navigating their databases to identify or mine required information. If information is not kept in a well-structured format, the ability of the vendor or company to mine data and provide clear, accurate, and timely information will be considerably impaired and may be prejudicial to the company's success in future contract bids. In addition, much of the information gathered during the conduct of a program is used in new proposals and other areas. Being able to manage and source this critical information permits effective bidding on new work. It is in the interest of the company to ensure that its subcontractors' databases are well organized and can be mined for information once a contract is completed.
- *Timely reporting of serious incidents/matters*. Consultants are required to provide timely and accurate reporting of serious incidents or matters in order to permit the provider's management team to implement effective control measures, as well as to notify the appropriate company management staff. However, consultants might be so focused on dealing with the incident that they forget that other crisis measures are required and that corporate management discussions between the vendor and company corporate offices are also required. Due to poor information integration or transmission, company corporate and program managers have on occasion been embarrassed by not knowing that serious issues or incidents have occurred. Establishing an effective reporting system helps both the company and the vendor conduct more efficient business.
- *Honesty with clients*. Consultants lying or misinforming project staff on matters that should be transparent undermine the company's confidence in the vendor's personnel and threatens the vendor's reputation as well as the actual contract.

- *E-mail chains*. Consultants forgetting that their response to an e-mail will have a chain of previous e-mails attached can lead to inappropriate or embarrassing information being made available to the company or other inappropriate parties.
- *E-mail content*. Including inappropriate comments or suggestions in any e-mail related to a contract might present challenges during an audit or review for both the vendor and the company. Any offhand e-mail comments may be taken at face value, unintentionally placing the vendor at reputational risk or inaccurately suggesting inappropriate actions were taken, thus incurring fraud or other investigations or allegations against the company.
- *Understanding who holds budgetary control*. The consultant must identify who in the company's structure has budgetary authority and must accept authority to proceed with services only once confirmed by these appropriate parties or persons in a contractually valid and legally binding request. Documentation provided by an individual lacking budgetary authority will not permit the billing of services to the company, placing the vendor at risk.
- *Failing to offer options*. Consultants may fail to identify innovative solutions that might enable activities to occur. Project management staff should always feel that the consultant is attempting to solve problems, however difficult or even costly the solution might be. The company will view the consultant, and by extension the vendor, as a hindrance to operations rather than a facilitator to success if options supporting its needs are not provided.
- *Failing to explain and document task refusals*. When a task cannot be conducted due to unavoidable risk or other factors, the consultant must support the rationale behind the refusal with documented evidence. A lack of documentation calls into question the decision process used to refuse services to the project. It is imperative that the company clearly understands why the task cannot be conducted; otherwise the company may conclude that the grounds for refusal are unsubstantiated, rather than being based on an accurate and well-founded risk assessment. This situation may call into question the consultant's competency and be a liability to the vendor's reputation as well as to the intercompany relationship.
- *Contentious e-mails*. Consultant's sending contentious or heated e-mails that can never be recalled, or that may be sent to persons to whom the consultant never intended, undermines business operations on multiple levels. In addition, the recipient (or others) might use such e-mails out of context, or to support their own agendas, undermining the consultant, the vendor, or indeed the company.
- *Taking sides in an intra- or interclient dispute*. The consultant should always attempt to remain neutral in any dispute within a company's organization or between two managers. The final outcome of an argument between project staff is never certain, and the consultant might be accused of a lack of loyalty or professionalism if on the losing side. Vendors should always be impartial and only offer clinical and well-founded advice and guidance.
- *Not retaining accurate documentation of contract changes*. A contract will invariably change over time as different variables alter the nature of services provided. This is normal. However, e-mail records do not accurately capture fundamental changes adequately. These should be formalized for confirmation with the company as well as for historical reference. Failure to do this can create a breach of contract or disrupt effective

billing. Retaining accurate documentation is particularly necessary for back-to-back (job-sharing) positions where consultants must understand and explain to the company the rationale behind such changes or decisions.

- *Applying inappropriate management approaches*. Consultants who have recently left a particular field after many years may habitually apply known management approaches, standards, and logic that do not always fit into commercial or specific project operations. Although consultants will have been selected due to their background, knowledge, and experience, it is essential that they understand that different drivers regulate the commercial sector and that applying out-of-place or inappropriate logic can undermine the contract or business activity.

Some examples of how consultant errors have negatively impacted contracts and operations follow:

- *Speaking of specialist areas without the relevant experience*. During informal discussions, local project staff asked a close protection team leader questions regarding electronic countermeasure (ECM) equipment. The team leader used out-of-date information based on prior military knowledge (nonspecialist), which then undermined efforts of the company's security director to procure ECM equipment, impeding risk mitigation efforts and damaging the company/provider relationship.
- *Offering services without contractually binding documents*. Armored vehicles were rented to a company for several months without contractually binding documents. When invoices were produced sometime later, the company insisted that the use of the vehicles had been a favor, not a cost service, resulting in a significant loss to the vendor.
- *Applying inappropriate management approaches*. An operations manager making an error on leave rotations opted to consider morale before service delivery and planned to stand down a monthly contracted service for two days to permit personnel to go on vacation. This would have had direct cost impacts on the contracting company for paid-for but used services and also would disrupt project requirements. Had the manager followed through with his flawed decision, it would also have placed the vendor in contractual breach.

Risk consulting and security management services form the foundations of successful corporate business continuity and are a central management component for convergence within any organization. Risk consultants and security managers are often responsible for determining how security services are planned, resourced, and conducted. Experienced vendors will provide to companies consultants and managers who understand the different requirements of these two distinct fields as well as those who can bridge the gap and conduct both concurrently. Companies seeking to own in-house risk and security resources should leverage their security professionals in order to support risk management, business enterprises, and operational planning for projects. Selecting qualified and experienced risk and security managers, either from external vendors or as part of the in-house organizational structure will enable better corporate decision making and more productive business results.

It is also important for contracting companies and their subcontracted vendors to understand the need to include specialist support at the right point within a business cycle as well as how to develop a mutually beneficial intracompany management and operational

relationship. The objectives of the consultant or manager should be clearly understood and, where necessary, documented to solidify agreements. In addition, the skill sets and competence of each post should be scoped and defined to ensure the avoidance of errors that can impact both the company and vendor. Understanding the common errors made by management, both within the company and by the subcontracted consultants, will also enable projects to mitigate both business and operational risks.

This book addresses in detail both areas of consultancy and management services and the peripheral requirements associated with both: that is, the services that they directly manage. Readers should remember that there is no one answer to the issue of how security consultancy and security management should be conducted, as each company, business activity, and environment will be different. However, the aim of this book is to provide the foundations upon which individual and unique requirements can be based.

Note

1. For simplicity, the term *consultant* will be applied to the functions of both a security manager and consultant, unless stated otherwise.