Corporate Security Challenges

By Ching Eng Leong

1. Introduction

Globalization has changed the structure and pace of corporate life; the saturation of traditional markets is taking companies to more risky places; the shift towards knowledge economy is eroding the importance of 'place' in the business world; new business practices such as off-shoring, challenge companies to manage at a distance; and new forms of accountability, such as corporate governance and corporate social responsibilities, put added pressure on companies to match their words with deeds, wherever they are operating.

At the same time, security risks have become more complex, too. Many of the threats, such as terrorism, organized crime and information security, are asymmetric and networked, making them more difficult to manage. The world is borderless today. There is also greater appreciation of the interdependence between a company's risk portfolio and the way it does business: certain types of behavior can enhance or undermine an organization's 'license to operate', and in some cases this can generate risks that would not otherwise exist. As a result, security has a higher profile in the corporate world today than it did many years ago. Companies are looking for new ways to manage these risks and the portfolio of the security department has widened to include shared responsibility for things such as reputation, corporate governance and regulation, corporate social responsibility and information assurance. Corporate Security Managers are required to enhance their skill to manage this borderless world today.

2. Characteristics of Alignment – Needs to Know

There are six characteristics of alignment between security and the business:

1. The principal role of the security department is to convince colleagues across the businesses to deliver security through their everyday actions and decisions – not try to do security to or for the company.
2. The security department is in the business of change management rather than enforcement and works through trusted social networks of influence.
3. Security is there to help the company to take risks rather than prevent them and should therefore be at the forefront of new business development.

4. Security constantly responds to new business concerns and, as such, the portfolio of responsibilities and their relative importance will change over time. Security departments should never stand still or become fixed entities. In many companies today, its role is more concerned with overall corporate resilience than 'traditional' security.
5. Security is both a strategic and operational activity, and departments must distinguish between these two layers.
6. The power and legitimacy of the security department does not come from its expert knowledge, but from its business acumen, people skills, management's ability and communication expertise.

3. Core Elements of Corporate Security

As a professional security to be exposed to corporate world, we need to understand the core elements of corporate security for us to execute our responsibilities. The following are some of the core elements of Corporate Security:

- Personal Security
- Physical Security
- Information Security
- Corporate Governance
- Compliance and Ethics Programs
- Crime Prevention and Detection
- Fraud deterrence
- Investigations
- Risk Management
- Business Continuity Planning
- Crisis Management
- Environment, Safety and Health

4. Understanding the Roles of Corporate Security

For many years corporate security has been dominated by a 'defensive' approach, focused on protection and loss prevention. The head of security was seen as little more than the 'guard at the gate', someone whose actions invariably stopped people doing their jobs instead of

enabling the business to function more effectively. Typically, heads of security came from a narrow talent pool, namely police, armed forces or intelligence.

There are many reasons companies tend to recruit security managers from these backgrounds. The police and armed forces churn out individuals with intensive training in the practice of security and protection, and have hands-on experience that is rarely available elsewhere. There are a number of reasons greater diversity is essential within the corporate security function.

1. There is a growing recognition of the strategic importance of security and as a result security departments need to operate at a much more senior level.
2. Matrix organizations require a particular approach to management and leadership, which can be antithetical to those with police or armed services backgrounds. In today's corporate environment, the impact of the security department is proportionate to its ability to persuade individuals and teams all over the company to collaborate and cooperate. This means that dialogue between security specialists and non-specialists is essential.
3. Traditional security skills are associated with an approach where security is perceived as a 'dis-enabler' of business. Those with formal security training can tend to be risk averse, while businesses need to take calculated risks to stay ahead of competitors, break into new markets and maximize profits.
4. The corporate security function needs people who are happy breaking rules, innovating and thinking outside the box. Studies of security-related professions such as the police, the ambulance service and local authority emergency planning departments have suggested that 'too much' experience in a traditional security context can inhibit people from making innovative responses to security incidents. Heads of security consistently rated qualities such as independent thinking, willingness to challenge assumptions and behaviors and innovation as being ones they value most in their team. One will say: 'I'm looking for people who push the boundaries and constantly challenge the way we work.'
5. There is a growing recognition of the value of 'the human element'. According to experts, many security professionals are typically trained to address security incidents and emergencies in ways that fail to factor in the human dynamics of such situations, including the impact of emotions, perceptions and fear on people's behavior. Emotional intelligence is critical to effective alignment, but the human element of security and risk management is routinely overshadowed by the emphasis on technical security skills.

For security to be aligned with the business, security managers must understand the business and how they contribute towards its objectives. The Chief Security Officer (CSO) is the

corporation's top executive who is responsible for security. The CSO serves as the business leader responsible for the development, implementation and management of the organization’s corporate security vision, strategy and programs. They direct staff in identifying, developing, implementing and maintaining security processes across the organization to reduce risks, respond to incidents, and limit exposure to liability in all areas of financial, physical, and personal risk; establish appropriate standards and risk controls associated with intellectual property; and direct the establishment and implementation of policies and procedures related to data security.

5. Challenges in Corporate Security

Corporate culture has a big impact on a security department. Often a company's culture dictates whether the security department emphasizes service or focuses on enforcement and control. Understanding a company's corporate culture will help identify how to structure a security department's role within the corporation.

Functional culture/facilities model

The functional culture is traditional and hierarchical where bosses boss and workers work. It relies on proven methods to serve existing markets, establishing clear work processes and respecting the chain of command. In this environment, security departments tend to be primarily concerned with maintaining the status quo. Departments tend to follow the facilities model — energy is consumed in the physical protection of the organization with such functions as guard operations and access control.

Traditionally, security has followed this functional culture with a military command structure. The general role of the security manager is to provide consistency while staff carried out their expected responsibilities. There is little room for advancement or for security to be involved in more than the physical protection of the facility. Whether the functional structure fits in well in many modern companies in a variety of sectors is open to debate. In non-traditional work environments, employees are moving away from — or not participating in — this traditional work setting.

Process culture/operations model

In the process culture, customer satisfaction and continuously improved operations are the primary goals. It relies on increased customer focus with emphasis on providing a number of specialized services.

Within this culture, security departments are designed on the operations model. This model brings added value by assisting in investigations, and providing a system design group, console operations, a safety unit, executive protection and administrative support staff.

The process-based culture lends itself well to the modern security department. It calls for cooperation between management and staff with its team emphasis on work. Staff members are expected to provide a high level of service to customers without constant attention of the security manager. The manager now performs a far different function wherein he or she acts as a two-way conduit between senior management who desire general security precautions and guidelines to be carried out, and the front line security personnel who are charged with the responsibility of carrying out general security duties. This process-based security manager is also expected to keep senior management apprised of upcoming security issues requiring attention. This structure is like an hourglass but instead of sand, information flows from one chamber to the next back and forth on a regular basis. Additionally, security personnel provide expertise in several areas, across departments and ranging from line operations to the boardroom.

Global companies face a significant cultural and legal challenge when dealing with security across international borders. Just as the European Union privacy regulation conflicts with United States laws, other regulations conflict between countries. It was once said that business is like a car traveling on a road to the business goals. The board of directors or senior management is the driver of the car. Management sets the speed, distance, and timing of when they reach their goals. How does information technology fit within that metaphor? Information technology would be the tires on the car that allow the management to drive on the road to

those goals. Information technology must keep good tread on those tires, maintain appropriate air pressure for the road conditions, and reduce potential tire failures from both internal and external conditions.

Regulatory compliance and data security is a very big issue when dealing with information technology whether it is local or national, and international companies face daily. This includes every type of business (public and private), non-profit, and governments. Security incidents can be initiated by internal or external forces from anywhere in the world, a global concern. Global issues face both national and international businesses. Global economy boundaries have been muted in the past few years with the advent of the internet. Each country has created laws or regulatory requirements for the different industries. Treaties have been established between countries, under international law, to provide an agreement on particular subjects.

When looking at legal and regulatory requirements, they have common thread to address issues stemming from fraud, theft, and malfeasance, from both internal and external threat actors, of a particular data set of information. These threat actors could be located anywhere in the world. Increasing data-breach reports have shown the gaps and holes in the security posture of a company. Criminal organizations are using these security shortfalls to gain sensitive information for profit.

Malsec Dot Com 2011.