Concerned About Physical Security and Safety?

The physical security and safety issues need to be addressed dynamically with progressive use of evolving technologies.

● **SUBMITTED BY** *COL RS BHANDARI, FOUNDER & PATHFINDER, MARGDARSHAN ADVISORY & CONSULTANCY SERVICES*

Col RS Bhandari,
Founder & Pathfinder
Margdarshan Advisory & Consultancy Services

WHAT IS IT?

The traditional approach to physical security comes from the military. It is guards, guns, and gates. The idea is simple; it places obstacles in the way of intruders, uses armed/unarmed guards to control access through fixed entrances and checking entrants for their admissibility. Over time complementary technologies have been added to increase obstacles and extend the view of the guards beyond what they can see with their own eyes.

The best definition I could find for physical security is available from the United States Geological Survey: "There is no object so well protected that it cannot be stolen, damaged, destroyed, or observed by unauthorized individuals. A balanced security system provides protection against a defined set of threats by informing the user of attempted intrusions and providing resistance to the would-be intruder's attack paths (USGS, 2005, p. 12)."

The first part of this definition is common to all security efforts; we cannot stop a highly motivated attacker (lone wolf). It is in the second sentence of the definition that we find the objectives of physical security. Putting it another way, the purpose of physical security is to delay an intruder's advance toward a target long enough to detect and respond with human intervention.

HOW MUCH IS ENOUGH?

In my last assignment in Mumbai I was often asked, is security adequate or is our organization safe? There is no cookie-cutter answer to this question. Moreover, safety is also about perception - how safe I am, as against how safe the place is? The short answer is that the sky is not going to fall, but we are not bullet proof. Security is always too much and never enough. The adequacy of security ultimately has to be determined by asking number of questions to the top management and not the Security Head.

For example, locks and possibly even a burglar alarm at your home ensure that your belongings are secure from all but the most well organized thief, but just using those to protect a bank is not nearly enough.

As a professional I feel adequacy of security must be assessed within the framework of four factors; threat environment, work ethos/culture, affordability and enforceability. In its implementation there should be uniformity, fairness and transparency which make it acceptable by one and all. Exceptions should be barest minimal, if unavoidable.

IT'S DYNAMIC

The level of adequate security as outlined here is constantly changing in response to business, risk environments and the variation in risk tolerance that management is willing to accept. This is a continuous process, not a final outcome. In simple terms be alert, review it as often as desirable, to be always safe.

Banking Security Convergence of CISO and CSO Functions

Purvesh Gada,
PwC,Associate Directo, Strategic Threat Advisory Services

The threat landscape has changed considerably over the last few years. Nowadays, the management of physical, investigatory and info security functions are highly interwoven and could be handled by the same person itself. And corporate security is heading toward this direction already. This has been a topic of discussions over the last few years, but now we can see large organizations heading down that path too.

As a trend, many companies are consolidating the CSO and CISO functions into one single function. Global banks are the front runners in adopting such trends. A few banks have already converged both these roles, which reports directly to the chief operation officer.

Regardless of what title these individuals hold, the important factor is that all security and risk management will be under one roof. Future security leaders will be more technically inclined than they are today, as that would then be the irreplaceable requirement of the job.

During last few years, the corporates (specially, Banks) have learnt the importance of security, and are making it an integral part of holistic business strategy. The heads of security are also being made a part of the decision-making process for the business as a whole. Risk as a function, containing both CISO and CSO will gain more weight in the next few years, which the banking industry has already started adopting.