("INDUSTRIAL SECURITY ISSUES - A Business Solution Approach"on 26 and 27 July, 2004 at Hotel The Gurney, 18, Persiaran Gurney , 10250 Penang, Malaysia)

Security Culture - A Mindset for Management and Staff

(Presented by Ramli Bahari, Principal Consultant MALSEC DOT COM)

Ladies and Gentlemen,

Let me begin this session by **introducing a familiar situation** in our work environment. **(Slide1).** A speaker comes up to the rostrum, feebly taps the microphone once, twice and assured of its functionality, began his speech. What has actually transpired?

In that short span of time, there is doubt lingering unconsciously in his mind about the microphone, not testing the credibility of the organizer. The organizer is equally concern about the outcome of such action. To date I have yet to encounter any organizer who has been offended by such action. This is because they **share the same culture of security**. It is an excellent example of security culture in action.

I am sure you have seen this happened at many functions or events. A practice that has consistently being adopted that it has evolved into a norm, subsequently into a culture. It is not the tapping actions that really mattered but most importantly, the activities in the subconscious mind. Every security practitioners are familiar with this phenomenon of Murphy's Law. **(Slide 2 and Slide 3)**

In its positive perspectives, this concern invariably has always being the forefront in the mind of most security practitioners. This is good because one of the unique security behaviors is the ability to anticipate problems and response pro-actively.

With that preamble, I am going to cover the **topic in 4 parts (Slide 4)** as follows:

1. **Culture of Security Defined** and critical **factors** that help in the **development of security culture.**

2. The **people that adopt and practice security culture**, highlighting the different **environment and its contrasting objectives.**
3. The **events and activities after September 11** that could influence to **shape the new security culture**.
4. My opinion in respect of the security culture.

Ladies and Gentlemen,

What is a culture?

Culture is equal to collective behaviors over time frame of about 5 years.

What is a corporate culture?

In the corporate world, **it is the practiced interaction within the organization**, be it in the boardroom, operational or backroom support units over a period of time.

- The culture in a way depends very much whether it is foreign or local base. If foreign base, certain behavior or actions are **transferred or imposed by** the culture of the principal company.
- That is why the **working environment** in the multinational companies varies according to the cultures from the country of origin.

What is Security Culture?

- A culture of security implies the **adoption of new ways of thinking and behaving when using and interacting within a community.**
- It is a **subculture** with certain set of similarities and differences in its values
- The practices could either be **overt or covert** depending on the objectives.

- It is **driven by time, major events or outcome of significant events or tragedies and perception**. (The lighter story – Slide 5)

What elements help in the development of the culture?

Developing a culture of security within a corporate environment depends on **company core values, ethics, leadership and effective awareness communications.**

- The **core values** determine the thinking which influence the behavior towards a positive or negative behavior i.e. respect for people is a belief that promote good security culture.
- **Leadership** is when the influence comes from the top as part of the corporate vision.
- **Effective awareness communication** is when it is systematically promoted as the corporate program.

Ladies and Gentlemen,

In wider perspectives there are **5 categories of people** (Slide 6) that adopt the so-called culture of security with its totally **contrasting objectives.**

This first category is the people who work, support or serve as **government officials in the government or its agencies. This includes the corporate people** whose business success depends on the political and economic stability of any nation.

- They can be classified as the **loyalist and supporter** to the system. They conscientiously enforced the law in order to attain a favorable business environment.
- This category prophesies **harmonious relationship and goodwill** with a clear objective to combat evils in order to live in a more peaceful world.

In the **underworld**, we have heard the familiar terms such as the 'Silent Empire' and 'Code of Silence' or in the local environment 'One- One' and Two-Two'. These second category include ex-convicts or recidivist as well.

- Their famous **axioms in confidentiality** include 'The only way to keep a secret is to say nothing' and 'Every thing leaks'. People talk everywhere and even in their sleep. They do not trust anyone.
- These are actually the underground security culture observed by the organized **syndicates or gangsters** e.g. syndicates etc.
- **Mistakes made will be punished severely** through elimination or made to retire, retirement in their world means stop living.
- Their main objective is **profit at any cost through power for total control and domination.**

The third category is the people who have constantly claimed to work towards **creating a better world**, regardless what political system in place.

- The categories called themselves by many names such as **liberationists, revolutionaries**, certain NGOs etc.
- The groups **may advocate or utilize** sabotage, theft, arson, militant tactic, associated with civil disobedience. Their adoption of security culture is to **defeat counterintelligence operation by the authorities** that would disrupt their activities and ability to evade arrest.
- Their definition of security culture is people **should know their rights and most importantly is to assert them.** They employ this tactic when detained by the authorities.
- Their stringent practices include
    - Not only switching off handsets during meeting but also to **remove the battery** as well.
    - They focus on **educating the new members** and will not antagonize them even when they make mistakes.

The **fourth category** is the **general public** i.e. others members of the public not included any category mentioned.

- Generally, the community **depends on the measures taken by the government** to provide the necessary protection from the criminal elements.
- However, through awareness campaigns, they also developed their **own culture of security by taking measures** to protect
    - Their personal safety and well-beings inclusive of their properties i.e. **alarms, grills, pepper spray, body guards etc.**

- The law-abiding citizens would not even think leaving their houses **without their identity cards** or driving licenses.

The fifth group that is compelling to mention is the **security people i.e. security practitioners & professionals**. The culture within the security community itself is unique in the sense that this group comprised of **ex-services people** either retired or still actively serving the private sectors or involved in security related business.

- The security practitioners strive to promote the **climate of honesty at workplace** as a form of desired culture of security in their environment through education, awareness and enforcement of rules and regulation.
- Continuously promoting the slogan **'Security is everybody's business'** despite everyone continue to believe that security is still accountable.
- Constantly promoting and reminding of good ethical practices standards that **keep people to remain honest or least avoid unethical practices.**
- The security practitioners strive to enforce rules and regulations that are often unpopular.
- There will be **no compromise on universal values of trust, honesty and loyalty.**
- Security leadership often **visible in times of crisis.**
- They are blessed with unique **blend of security culture** (police-military & civilian) with continued interest in crime prevention but not getting the opportunity to be involved.

Ladies and Gentlemen,

Therefore, it is now appropriate that we look at 'Security Culture' from two perspectives i.e. one that is era before and after the tragic event of September 11.

September 11

I received the call from one of the crisis team members on the news of the attack whilst on a holiday in my kampong. Immediately, I got into the net and there in the CNN news, tragic event was continuously repeated

highlights throughout the night. I packed my things and got the family together back in the city the next day.

The family members in the kampong could not comprehend this sudden change of plan. **'After all this happened in the US and they truly deserved it'** was their first reaction. **A traffic accident at the kampong road was more heartrending then this faraway tragedy.**

Back in the office, business was as usual. The security personnel were **excited, plenty of speculations but told to be extra vigilante** as that was an American based company. Alerts after alerts came from the corporate office and US embassy.

Today the **phrase 'September 11'** needs no further explanation. It has evolved so quickly to become part of the security culture with more synonyms such as 911 and most recent Fahrenheit 911.

Going through the various reactions helps **us understand the elements that influence the new developing culture in security**. It was further discovered that the existing security system did not contemplate terrorists **willing to give up their lives during an attack.**

This horrific event changed the landscape of security in many countries in the world. Increase visibility and devoted budgets in security services for government agencies. The immediate concerns were high-rise building occupants and of course aviation security.

- ASIS International's recent survey of security officials at some of the largest corporations revealed that corporate security spending only raised a median of 4 percent since the 2001 terrorist attacks. Security spending has increased so little because of the economic downturn and companies' need to reduce spending to maintain stable bottom lines. (Washington Post 2003)
    - Prior to September 11, in order for security to appear as **perfect business partner**, it has to be seen cost effective at every move. Allocation of financial resources invariably was based on **return-on-investment.**
    - **No new is a good news** was the measurement metrics to gauge the success of security in the early days. This concept of everything is in good order with terminologies such as **'All quite in the frontline' or 'Baik Adanya'** were widely accepted as the norm by security practitioners and professionals.

- I remember just prior to September 11, the term **'good to have' versus 'nice to have'** took precedents to become the standard of the day. Security comes at a price forgetting that negligent in security comes at a much higher price.

- Out-sourcing the security was the strategic business decision. It was then a question whether we can live with what we have. It is not a question of whether we can afford it but it's a question of whether we can afford not to have it. Therefore in that context, we need to find whether **out-sourcing the security function is the right formula**.
- I guess the trouble with the security practitioners was that we were unable to equate security to actual bottom-line saving. More so, **we were not able to put enough 'fear factor' to the management** (Slide 7) because we did not the model to demonstrate the impact seen in the tragic event of September 11.
- (Slide 7-a) 18 years ago this guy made a press statement about snatch thieves in George Town. **The media did not place much 'fear factor' as it is today**. Back then the suggestion was not too good because it was probably not favorable to the related industry.
- Slide 7-b) The sad thing about the image of the security profession that it may become a culture if unchecked. The **criminals will see this weakness an opportunity.**

- In aviation security, we saw the **introduction of air marshals, 100% passenger and baggage screening and restructuring flight decks** etc. In short the security program begins at the **point of ticket purchase.** The program may include security system with built-in redundancy in the sense that multiple checks are required. Singapore Airline has also had their air marshals in place.

- Biometrics verification, where geometric measurements of a **person's face or hand are used as the standard identification** procedure at airports in the United States. Biometrics could **speed travel by ensuring that everyone on the plane is supposed to be there, and by helping to verify airline workers' identities**. Some potential passengers believe it would be an invasion of privacy, while others see it as a necessity in keeping airlines safe. (El Paso, 2003)

- Airline carriers are **installing hidden cameras** on commercial flight. This **allows pilots to monitor cabin activity** from the secured cockpit, although privacy issues have already started surfacing. Jet Blue Airways has cameras on all their planes, and United Airlines is reviewing tests results from camera trials, before they decide whether to install more or not. (Wall Street Journal, June 2003).

- Corporate travel departments have revamped their systems to focus on **educating employees about the risks** of traveling abroad and how they should act if faced with a **dangerous situation**. They also urged employees to stop making their own **travel plans via the Internet**. (New York Times, 2003)

- Los Angeles officials announced that the city's international airport would be rebuilt to incorporate new security measures to prevent **terrorists from entering the nation**. The city plans to prevent passengers from **driving up to the airport** to prevent the use of car bombs. Experts note that 80 percent of the airport's airlines are opposed to the measure. (USA Today Online, 2003)

- The Sept. 11 terrorist attacks have forced many companies to implement life-safety initiatives for their **employees of a high-rise building. The life-safety team focused on creating a comprehensive evacuation plan** that would be readily available to all employees. The team discovered that cell phones were an unreliable form of communication during the chaos of evacuation. **Phones with walkie-talkie feature are preferred communication tools during an emergency**. (Security Management Vol. 47, 2003)

- Planning, training, and frequent drills should top any company's or building manager's list of necessary safety improvements. Experts advise that buildings should have set **procedures for security guards in case of an emergency; include considerations establishing warden, overriding magnetically locked doors & elevator recalls**. Drills should include fully test evacuation skills and performance evaluation. (Security Management. Vol. 47, 2003).

- For aesthetic appeal, companies often look toward **"transparent security," which is briefly defined as unobtrusive or hidden solutions to potential security problems.** For example, during the Sept. 11 terrorist attacks on the World Trade Center, several people **were killed or wounded by shards of flying glass.** These deaths and injuries could possibly have been prevented if the buildings' glass panes had been treated with a type of **"fragmentation-retention**

film" that prevents glass shards from flying through the air when impacted. (Access Control & Security Systems Vol.46, 2003)

- **Armed soldiers perching on a military vehicle with an automatic weapon**, and intimidating jersey barriers dotting city sidewalks and road ways, its easy perceive the measures as scary, With the new security scare Washington officials began looking for ways to make security invisible but present, in order to preserve the integrity of the city, and its historic buildings. (CSO Magazine, May 2003)

- Closed Circuit Television is getting a surge of new technology to develop methods of intelligent imaging and software that would allow cameras that are **producing high resolution images to detect motion, become IP addressable, and track an object throughout a building,** even when there are other people or object present. In more extreme situations, cameras are being built with the ability of a camera to be cause non-lethal harm to catch intruders. (not yet in use). (Security Management, May 2003),

- **The canine explosives-detection industry has blossomed** since the terrorist attacks of Sept. 11, 2001. Dogs have an incredible sense of smell, and are accurate at detecting a wide array of explosive substances. Companies can invite law enforcement teams to their facilities to participate in security or anti-terrorism exercises, Companies benefit from these **exercises because the canine units and law enforcement teams will become familiar with a company's facilities,** which could prove helpful in the event of a real emergency. (Security Management Vol. 47, 2003).

- Policy Matter, a company specializing in corporate compliance, believes that temporary workers on short-term assignments pose a great security threat if allowed to access sensitive systems such as email or the Internet. **Temp workers are a risk because they are often not informed about company security** policies and may unknowingly put the company at risk for a computer virus. (Silicon.com, June 2003)

- **Identification checks, high-tech security cameras, and other devices may be the norm in New York City, but in Dallas, San Francisco, and other large U.S. cities, security is not always a top priority.** Despite these figures, slews of buildings around the nation seem to have no more security today than they did before the attacks. Building managers in Los Angeles and Washington D.C. says that, despite a keener awareness of terrorist threats, office tenants

often opt against tighter security, which can become inconvenient and costly. (New York Times, 2003)

Ladies and Gentlemen,

Let me concluded this session with FIVE important observations.

1. **We have taken many actions in term of security measures but we are no safer than before**. The security practitioners in general have to continue promoting the elements of sensitivity amongst his team members and their associates in order not to get into a catch 22-situation. Despite of phenomenal increase in cost of security and safety, the general public does not feel any safer.
2. We have learn new consequences of horrific **events or happenings around the world that will influence our thinking, shaped our behavior and actions that will eventually developed into the culture of security.** Suicide bombers and car bombs are the trend in today's terrorism.
3. The security practitioners who include the service providers, system providers, private **investigators can make significant contributions to the society in terms of crime preventions at various institutions, factories** etc. in the private sectors but most unfortunately, their resources and potentials have been neglected by the relevant authorities in crime prevention efforts.
4. Finally the **criminals on their own have developed their own security culture to minimize the chances of being apprehended.** Therefore it is most appropriate that the authority to do differently by developing a different strategy to get the right result. It takes extra-ordinary effort to get extra-ordinary result (Slide 8).
5. The security industry really **needs help from the press** and media.

With that thank you for your time.

26th July 2004