

Business and Industrial Security: Past, Present and Future

Bertus R. Ferreira

Criminal Justice Program, Murray State University, 101-S Applied Science Building, Murray, KY 42071-3345, U.S.A.

E-mail: bertus.ferreira@murraystate.edu

Security Journal (2007) 20, 31–34. doi:10.1057/palgrave.sj.8350042

When I joined the American Society for Industrial Security (ASIS) in 1982 and became the founding Vice-Chair of the first ASIS Chapter in Africa, business and industrial security in the Republic of South Africa was very much focused on/towards armed robberies and terrorism. South Africa was experiencing a daily threat of terrorist attacks from indiscriminate and vicious killers armed with AK-47 machine guns, bombs and Russian land/tank mines. Civilians at bus and train stations, farmers in remote border locations, banks/financial institutions and business and industrial employees were the favourite targets, and security was geared towards target hardening, access control, and using highly trained and heavily armed security officers for protection.

When I arrived in the U.S.A. in November 1983, I found security concerns in the U.S.A. very different and mainly focused on issues like espionage, shoplifting, employee theft, fraud (discount coupons, checks, credit cards) and trying to prevent costly law suits. The CPP examination that I took and passed in June 1984 was totally slanted towards the U.S.A. with numerous questions on law, all of which were based on U.S. legal principles and U.S. Supreme Court rulings. However, since then ASIS and the CPP examinations have become more internationally focused.

As a criminal justice professor in Wichita, Kansas, from 1992 to 1994, I was told by various academics that my 1992 prediction that terrorism would soon make a major impact on the U.S.A. was based on my “foreign” background and that it had no reality to U.S.A. conditions. Faculty with social science-focused doctorates thought that the university (and I) should not waste time by offering academic courses on terrorism, but that we should rather cover the normal types of criminal justice courses in policing, courts, corrections and juvenile justice.

Even after the first bombing of the World Trade Center on 26 February 1993, the public at large did not believe that this was the beginning of severe terrorism events to follow in the U.S.A. Most believed that the foreigners who were involved in that event were just part of a small group of fanatics with no links to other international terrorist groups or countries. Also, most of the people in Kansas and the Midwest believed at that time that terrorism was just a problem for big cities and far-off places.

Of course, Timothy McVeigh proved them wrong in 1995 and the target was just 157 miles to the south of Wichita! However, although McVeigh turned out to be a home-grown terrorist, many in the media and some law enforcement officials were quick to think it was a

“foreigner” who placed a truck bomb next to a day care centre at the Oklahoma Federal Building. This sudden shift in the security threat was hard to accept for most Americans who thought that the Oklahoma City event was just an isolated incident. They forgot that the Unabomber, Theodore Kaczynski, terrorized the U.S. for many years. However, the fact that he killed so few people and so far apart in time and place did not seem to make him a threat to the mass population as such.

We now know better, but hindsight is 20/20. By 1995, most so-called terrorism experts (“talking heads”) on TV were people who had neither investigated acts of terrorism, nor arrested or interrogated a single terrorist. Neither the FBI nor the CIA, at that time, made the case for a world-wide terrorism onslaught on the U.S.A. and the general U.S. population could not be bothered, since they did not think terrorism would have a direct impact on them. What many people do not understand is that terrorism against the U.S.A. is terrorism against the economy and business environment of our society. The whole stock market and tourism/travel industry (airlines, hotels, motels, restaurants) in an open society and free market democracy are dependent on a terror-free economy. It is thus of utmost importance that business and industry join forces with the government to protect us all from potential terrorist attacks, even if it costs billions of dollars.

Business and industrial security will have to take current events into consideration, be very adaptable to the actions of criminals and terrorists, and try to stay somewhat at pace with criminals. The criminal justice system usually lags behind criminals and is rarely acting ahead of them with effective crime prevention measures. It seems that the future of business and industrial security will be dominated by the following main issues as discussed below: terrorism, transportation, technology, corporate/governmental corruption and debilitating lawsuits.

The war on terrorism is here to stay. Although the U.S. was not directly affected by terrorism on our soil until recently, some allied countries, like the United Kingdom with the IRA and Israel with the PLO, Hamas, Hezbollah, Islamic Jihad and others, have suffered for many years from relatively localized problems of terrorism. We should expect to see more attacks on U.S.A. soil, our overseas properties (embassies, businesses, factories) and against our international allies/friends for years to come. And yes, we will have our first homicidal terrorist bomber blowing himself or herself up in a busy public place – it is just a question of where and when. This will happen regardless of who is the President of the U.S.A., which party controls Congress, or how U.S. foreign policies are conducted. Extremist fundamentalists from around the world hate us and our allies, and they will continue to attack us whenever and wherever they get an opportunity. The naive idea that we can somehow negotiate with terrorists and reach some form of peace agreement with stateless enemy combatants stems from a lack of understanding and insight into real terrorism. We will also not be able to kill all of these terrorists, since new ones are born and indoctrinated with anti-Western ideologies every day. The best we can do internationally is to assist in minimizing poverty and conditions of despair in some regions of the world where fanatics use these sufferings to recruit new fighters to their cause. We will have to get more countries involved in closing down “religious schools” where only hate is taught, arresting and prosecuting local leaders who instigate violence among their followers, and find a more useful role for the United Nations to keep the peace among various warring tribes, cultures, races, religions and nations.

The U.S. transportation system is very vulnerable, from airlines to trains and beyond. Any school bus can become a target of terrorism anywhere and anytime in rural America. We simply cannot provide security at high levels on all buses. Also, it is estimated that only 5 per cent of container shipments are screened before they are opened in the U.S.A. Anything, from smuggled illegal aliens, explosives, nuclear material, biological viruses or chemical poisons may be hidden in the other 95 per cent that are not searched. This has become a big political issue and everybody wants to blame the other. The truth is, we currently have no technology or methods that would allow a 100 per cent screening of all containers without bringing the whole shipping industry to a halt! Furthermore, can we trust the foreign senders of all containers to search the shipment for contraband before sending it to us?

The future of security is closely aligned with computer science. One of the most troubling areas is the rampant increase in identity theft that can ruin the lives of unsuspecting people from a distance. The more technology is being developed and used by society, the more criminals will use that to commit crimes or harass citizens. The main targets have always been cell phones, computers/internet and high-tech electronics. One of our main challenges is that we are not even keeping up with laws to ban, punish or shut down internet crime. Just spamming emails alone are driving most citizens crazy on a daily basis! Child porn on the internet and unsolicited sexual advertisements in our work or private email in-boxes are two of the most obvious things that cannot be controlled effectively as of now. We need more research and development in the computer technology field to fight these problems; however, that does not seem to be the focus of many "cyber geniuses". Some of them seem more interested in creating new games and gadgets, while others spend their lives trying to hack into systems or develop viruses to attack computers. We, as a society, need to find ways to reward these "wiz kids" for developing measures that protect people from cyber criminals or cleaning up internet problems. New technology research is also desperately needed to develop efficient and cost-effective equipment to detect bombs, explosives and drugs.

Corporate and political corruption and fraud are creating unique problems for security. Recent scandals involving bribe taking, raiding of corporate pension plans, false accounting reporting, crooked auditing, insider trading, political influence peddling and soul selling, and greedy executives have made many Americans skeptical about the ethical values of senior people in business and government. Corporate insiders appear to neither look for criminals among themselves nor recognize corporate offenders. It is time that all business schools/colleges in the U.S.A. incorporate not only principles of ethics into their curriculums, but also more specific security and white-collar crime courses. The various business programme accreditation agencies should require courses about crime and criminals as part of their accreditation guidelines. Security managers need to become more aware of lobbyists or corrupt politicians, who may want to use their companies for financial gain. This appears to be a nagging problem in the government contracting environment, especially regarding defense contractors. They should also prevent company executives from making illegal, political campaign contributions with company money or from bribing politicians for legislative favours. It is time to restore the trust of the American public in business and well-qualified security managers are seemingly the only ones who could make that happen.

Our current society seems to be driven by lawsuits. We have been encouraged to believe that everyone should sue everybody for everything. Class action lawsuits has become the most popular form of business for lawyers who take the bulk of the money and leave many of the plaintiffs with very small settlements or just coupons for the same products. Ridiculous lawsuits have driven many good companies from business, increased insurance premiums, increased medical costs beyond what a normal person can afford, and have driven certain medical specialists (like OB/GYN) out of some communities who need them the most. These lawsuits have done little to stop the real criminals who prey on our society. Angry juries add to the problem sometimes by awarding plaintiffs unreasonable punitive damages for things that could hardly have been foreseen or prevented. Companies are often advised not to settle, but rather to fight claims. However, companies will have to pay legal fees whether they win or lose the lawsuit. For instance, if a company has a problem with a faulty product, they will sometimes resist a costly recall and instead try to fight lawsuits if they think that would be cheaper. However, in many cases, the massive lawsuits will eventually force them to do the recall anyway, and by that time, they have spent money twice for the same problem. The powerful lobbyists of the ABA have been very successful so far in blocking real tort reform that any President or Congressional reformer would like to introduce. In a democracy where politicians constantly have to run for re-election, nobody wants to offend the influential legal community. In this "sue your neighbor" environment, security professionals have an obligation to protect company assets by doing anything in their power to prevent company actions or negligence that could trigger large amounts of civil law damage awards. It is time that savvy security managers have the input at very senior management levels where they can advise companies to be more careful about faulty research and development. Companies want to make money and scientists do not want others to beat them to the market, so many new products are seemingly released without extensive safety testing. These unsafe products may devastate the financial health of a company and it is, therefore, a security and risk management issue to be tackled head on.

In conclusion, it is my sincere belief that security must be part of a comprehensive risk management approach for business and industry. Security should not be reporting to another risk management, personnel, finance, administration, marketing or manufacturing function, but instead be part of a separate risk management unit at the vice presidential level in the organization. Only when security, occupational safety, industrial hygiene, fire control/prevention, emergency preparedness and insurance are all working together to address the risks of a company in a logical, cooperative and unified way, can we help protect the bottom line of any corporation. Companies must train and educate more of their general and senior managers to be aware of security and risk management issues. More senior security personnel must be educated in accounting, computer information systems and investigative techniques against corruption and fraud. Only when security managers are well educated and elevated to positions that are senior enough to be taken seriously by the corporate CEO and CFO, will business and industrial security be able to directly influence company policy and gain the professional respect it deserves.