The Corporate Assets Protection Program of Elite Cigar Distribution International

Camille Acred

Steven W. McNally, MA, CPP, PSP, PCI, CFE

Contemporary Security Administration

Southwestern College
Abstract

The Corporate Assets Protection Program (CAPP) is the foundation to an organization’s security program. In order to have an efficient and cost effective CAPP the Chief Security Officer (CSO) has to decide which assets are critical and need to be protected. The CAPP is not standardized and will differ depending on the corporation and on the CSO. The CAPP consists of several fundamental components. These components must be able to be measured and can be done so with the assistance of a security metrics management program (SMMP). The CAPP must constantly be evaluated to ensure effectiveness. This is an ever changing program depending on the environment and executives surrounding the organization.
The Corporate Assets Protection Program of Elite Cigar Distribution International

In society today a business cannot be successful without an effective corporate assets protection program (CAPP). The CAPP is the foundation to any security program and involves the protection of people, information, and physical assets. Kovacich & Halibozek (2006) explain that the how and why of a corporation protecting its assets are institutionalized in a CAPP. There are so many threats possible today; terrorist attacks, severe weather, information security threats like insider threats and computer viruses. A business has to protect all of their critical assets and be prepared to recover from any type of disaster. A CAPP can be managed as a plan or a program. One of the main security drivers for the CAPP is cost. Asset protection can be an expensive endeavor. It is the responsibility of the Chief Security Officer (CSO) to ensure that their organization’s CAPP is the most efficient and most cost effective option. Kovacich & Halibozek (2006) state that the costs and benefits of a CAPP, in addition to the efficiency and effectiveness of the program, are difficult to measure. In order to do this accurately, a CSO needs to develop a security metrics management program (SMMP), which is described by Kovacich & Halibozek (2006) as “a tool for security management to use to assist in the evaluation of security processes for effectiveness and efficiency.” For Elite Cigar Distribution International (ECDI), which will be discussed in the next section, the six fundamental components of their CAPP will be presented, as well as the metrics used to measure them which help drive performance toward results. The six components presented will be: risk management, information security, operations security, physical security, emergency management, and Security Education and Training Awareness Program (SEATP).
Section 1: The Organization

Elite Cigar Distribution International (ECDI) is a mid-sized cigar distribution company with its headquarters (HQ) located in New York City (Manhattan). In addition to the headquarters, the company owns ten cigar bars throughout the world. There are four locations within the United States: New York City, Los Angeles, Chicago, and Las Vegas. Six are located in foreign countries: India, Saudi Arabia, France, Italy, Brazil, and Japan. ECDI has approximately 500 employees worldwide; approximately 70 personnel who work at the headquarters (40 of them being travelling teams), and approximately 40 at each cigar bar location. ECDI stores and distributes high-end cigars with the most exclusive being the His Majesty’s Reserve, made by The Gurkha Cigar Company. These cigars were created in 1996, and each box is made infused with an entire bottle of Louis XIII cognac. A box of these cigars (twenty) retail for $15,000, making them the most expensive cigar in the world. As stated earlier, ECDI also owns and operate ten cigar bars in locations across the world, “Cigar Bar.”

ECDI was founded by two men in 2000; they are still partners and co owners. They began the company as the Cigar Bar in New York City and slowly branched out into the business it is today. The CAPP of ECDI was nonexistent in the beginning. The extent of their protection measures were that they left no cash in the bar after hours (after closing), a friend hired on as a bouncer, and a baseball bat kept under the bar. They had essentially no employees and not very many assets they had to cover. As their business grew, they added more Cigar Bars in places around the continental United States, then a corporate headquarters and finally spread to cities abroad. This required developing an asset protection program essentially from scratch. Not to mention, about a year after opening the terrorist attacks of September 11th, 2001 occurred. This was almost the end of their business. However, the effects of the 9-11 attacks did give them a
heads up in the area of emergency management. Within five years the business had grown to the size it is today, not intending to get any larger with the intent of remaining extremely exclusive. A Chief Security Officer (CSO) was appointed at the corporate headquarters with a small staff of seven that also consist of the information technology (IT) department. Each Cigar Bar location has its own security manager/IT manager.

Section 2: The Corporate Assets Protection Program

As stated earlier, the CAPP can be viewed as either a plan or a program. CAPP development is the sole responsibility of the CSO and its perimeters will be entirely dependent on the organization itself. Kovacich & Halibozek (2006) explain that the first step in the development and implementation of a CAPP is to decide what is needed in order to manage the program. One way of figuring this out is to look at the daily problems dealing with security within the organization. Stated simply, “The CAPP is a tool to protect corporate assets and mitigate risks to the corporation. Ideally, the goal is to accomplish this objective in as effective and efficient a manner as possible” (Kovacich & Halibozek, 2006).

An SMMP is used to help measure your program effectiveness. An SMMP can also provide executives with a performance assessment of your CAPP, which needs to be done to prove the effectiveness of the program. In order to develop an effective SMMP, Kovacich & Halibozek (2006) recommend taking the following actions; identifying the security drivers, deciding on what must be accomplished, identify how the work gets done, and finally conduct a process analysis. From this point one can identify each protection component. Within the CAPP for ECDI, there are six. After deciding on the components, they will need to be analyzed to find out what drives that specific component and what exactly needs to be measured. After these
initial decisions you can go in-depth with each component, selecting which data gets collected.

A CAAP can’t exist without the identification of possible threats to the organization. This is done through risk management. Risk management is the manageability of a threat. Fay (2006) describes this manageability as the capacity to reduce the probability or impact of a risk. Risk management is a large process which involves many subtasks. Risk is managed by one of the following options: avoiding the risk, reducing the risk, diffusing the risk, transferring the risk, or accepting the risk. In regards to ECDI, the main risks are in the information technology area. Because of the diverse locations all over the globe, the threats are different for each location. For example, the New York original location was hit hard with the 9-11 attacks. The Los Angeles Cigar Bar doesn’t have as great of risk of terrorist attacks. The Japan location is at risk for more natural disasters and the corporate headquarters in New York has different types of threats than the Cigar Bars themselves.

Kovacich & Halibozek (2006), state that the best way to effectively measure risks in organizations are by using security surveys. Security surveys help to assess risks by identifying threats and vulnerabilities to company assets. One example of a survey I would conduct in relation to ECDI is a threat tracker. This tracker would be location specific and document any incident which had an adverse impact on the corporation. The tracker would essentially be the same document used by all locations, created by the IT department. In this document you could input the type of incident that happened and the effect the incident had. For example, there might be more incidents of money or merchandise theft in Las Vegas than in Chicago. In Japan, there might be more incidents of property damage caused from heavy rain or earthquakes. This tracker would enable executives to see exactly how much money they were losing and the cause. This
would allow the CSO to implement changes to the CAPP in response to the tracker. This would also enable the HQ to conduct a roll up of all properties, essentially allowing them to see if drastic changes need to be made; possibly closing a location or moving it as a result of losses to the company. One specific example would be for the Las Vegas location. This Cigar Bar has shown an increase of theft of merchandise in the last six months causing them to step up security procedures; using cameras, alarms, and more security guards.

A Security Education and Training Awareness Program (SEATP) ensures that all personnel within an organization are trained to protect the organization’s assets. The CSO is also overall responsible for this program. The SEATP has two functions; security awareness and the protection of assets (Kovacich & Halibozek, 2006). In order to make sure employees are aware of security policies and procedures; they have to first know that they exist. This can be done through education; briefings, pamphlets, and open doors for communication. The second function of how to protect the critical assets can be taught using the same educational processes; reinforced with reading materials or training aids (posters, pocket cards, etc.) that are readily available.

SEATP can take a good chunk of profit away from the company. Every lost hour of labor or production due to training has an adverse impact on the organization’s total productivity (Kovacich & Halibozek, 2006). Without proper management the SEATP can actually cost more than it benefits the company. One of the easiest ways to measure the SEATP at ECDI is using the percentage of employees trained. The goal of the SEATP within ECDI is to have all employees 100 percent trained in security awareness and in protecting company assets. All training is documented so at any moment anyone could pull a percentage of which employees were trained versus not trained. At ECDI the tolerance is never to be under 90 percent trained.
This is supported by a new hire program which would require all training to be complete before starting work. The only time this would fall below 100 percent is people falling out of tolerance for annual training requirements. Upon completion of all mandatory training, employees are required to sign an agreement stating that they have received all training and understand all policies regarding security and asset protection. In addition, this agreement would state that the employee understands that they are responsible for their actions and will be held accountable. This training database would be available at each Cigar Bar location and the HQ could also view a roll up of all employees in the corporation.

Physical security is an obvious component of any CAPP. This is because these are all areas that are visible; buildings, vehicles, merchandise, and personnel. Fay (2006) defines physical security as “a set of tangible elements that protect selected assets from damage, compromise, and loss.” The critical physical assets of ECDI are: employees, physical locations of the ten Cigar Bars and the HQ, cigars themselves, cash, and vehicles. ECDI has closed circuit television systems (CCTV), bodyguards, fireproof safes, locked cases for transporting merchandise, and a walk in humidor vault located within the HQ. These are all safeguards in place to support the physical security function.

One method I would use to measure physical security within ECDI is to conduct vulnerability tests. The areas tested would include the aforementioned safeguards; using both announced and unannounced inspections. The HQ is where the largest storage of merchandise is located. There is a giant walk-in humidor which is set up basically like a vault. In addition to this vault there is a security guard stationed at the entrance desk in our HQ. This HQ is located in an office building in Manhattan which has security guards at the main entrance to the building. ECDI is not that restrictive in whom it allows up to the HQ. It is difficult to get beyond the front
desk of the HQ if you don’t have an appointment. One vulnerability test would be to see if an insider, posing as an outsider, could gain access to the vault; during business and non business hours. These vulnerability tests could be conducted against any of our safeguards at any time; the results would all be documented and kept in a database. Once again, the frequency and type of failures of these tests would dictate if we needed to make a change to our safeguards.

Information security is one of the most important components of a CAPP in today’s society. Kovacich & Halibozek (2006) state that:

The protection of information in this age of electronic and digital information is more important, and more complex, than ever before. The loss or theft of information critical to a corporation’s products, methods or processes may be devastating. In this age of global competition, the importance of implementing a comprehensive program for information is critical and cannot be overstated.

Nothing illustrates this point better than the recent WikiLeaks incident. In this incident, over 200,000 government cables of over 180 countries plus a video (titled Collateral Murder) showing the accidental airstrike on Reuters journalists, were put on a burnt copy of a Lady Gaga CD-RW and given to a representative of WikiLeaks. These files were taken from a classified (secret) computer system in a secure area in Iraq, by a trained Army intelligence analyst. The damage this has caused is already enormous, not to mention that this will go down as one of the worst security incidents in history.

Information protection is expensive. Kovacich & Halibozek (2006) explain that because of this, you don’t want to try to protect all information; only protect that information which requires protection. In addition to the CSO at the ECDI, I would also appoint a security manager whose sole purpose at the HQ was information security. The CSO and security manager would have a
six person staff at the HQ. As mentioned earlier, each of the ten Cigar Bar locations would also have one security manager. These individuals would keep track of all attempted threats to the (IT) system; from the smallest violation of lending out passwords or passing sensitive information in unencrypted e-mails. There would be software that tags specific sensitive files and monitors their activity, hopefully coming up with numbers of which areas within information security need the most attention. This component would work hand in hand with the Security Education and Training Awareness Program (SEATP).

Fay (2006) defines emergency management as “the process of preparing for, mitigating, responding to, and recovering from an emergency.” Fay (2006) also discusses emergency operating plans (EOPs), which incorporate each anticipated type of incident into one composite plan. These plans cover everything from tornados to explosions. Mitigating risk involves trying to avoid the incident from happening altogether, while remediating risk is the process of trying to lessen the effects of the incident on the organization if it does happen Fay (2006).

ECDI would conduct Emergency Action Plans (EAPs) on a recurring basis (tentatively quarterly). Only executives and security personnel would be informed that they were scheduled. The EAP could consist of a tornado drill, fire drill, an active shooter, etc. This would allow for an assessment of our current procedures and allow executives to see how well the employees knew and executed them. ECDI would use the number of actual emergencies or incidents at each of the organization's locations to drive the Emergency Action Plan for that location. For example, the New York City Cigar Bar and HQ locations would have an extensive terror attack EAP, as a terrorist attack is more imminent in that location. The Cigar Bar (ECDI) was hit by the 9-11 attacks in 2001 and recovered, therefore they are more experienced in that area than a tornado drill, for example.
Operations Security (OPSEC) is the final component comprising ECDI’s CAPP. OPSEC focuses not on sensitive information, but sensitive activities (Fay, 2006). Using the WikiLeaks example again, the information that got out to the public was extremely damaging, but fell under the prevue of information security. OPSEC covers the actions that led to that leak; i.e., Bradley Manning using a disc to copy classified documents. Within ECDI OPSEC is not necessarily a matter of national security. However, every organization in its own way has activities that could be potentially damaging, whether to their reputation, or to the business itself.

ECDI has an exclusive, need-to-know client list. Clients of ECDI expect to be treated with discretion, and not to be subject to have their personal information shared. Discussions amongst members of the several Cigar Bars also don’t want to have to worry about their conversations being turned into gossip in the latest tabloids. ECDUI also has to keep their business competitive. They do deal with the most expensive cigar on the market, and people that don’t think twice about paying. There is no room for error or for any of their business secrets to get out, regardless of how insignificant they may seem to you or me. One way to measure your OPSEC program is to have all employees sign a non disclosure agreement as Fay (2006) discusses in his text. I would also have a rotation of someone assigned to walk around at the end of the day to see how many people have left sensitive information (along with any merchandise) on their desks or in plain view. The number of these instances would be tracked. The number of violations total would drive a change in our training program or frequency of training if need be.

In conclusion, one can see that even with a business dealing with cigars requires a thorough CAPP. Kovacich & Halibozek (2006) state that “each corporation is different and operates in an environment unique to them.” The CSO, being the individual primarily
responsible for the CAPP will influence the direction the program goes as well. The bottom line is that CSOs must develop the CAPP and use data and security metrics that work best in their own environment (Kovacich & Halibozek, 2006). After coming up with a CAPP it must constantly evaluated, as no security program can ever remain unchanged. Times will change and threats will change. In evaluating your CAPPs effectiveness you must ask; is it working as planned, how much does it cost, how can it be done netter and how can it be done cheaper.
References


