Aegis®
security design
Strategies for risk containment

Case Study: XYZ Corporation

Outsourcing the Management and Administration of Physical and Electronic Security Systems and Programs Saves XYZ Corp. 800% in Annual Recurring Costs

Brandon Reich | Vice President

327 Townepark Circle | Louisville, KY 40243 | t: 502.244.7304 | f: 502.244.7308
www.aegissecuritydesign.com

Executive Summary

XYZ Company (client's actual name protected for the purpose of anonymity) made the decision to outsource the management, administration and operation of their physical and electronic security systems and programs to Aegis Security Design's Security Support Center (SSC). SSC provides the following services for XYZ:

- Enterprise Access Control System Administration
- Centralized Photo ID Badging
- Service Management and Administration
- 24x7 Emergency Support and Help Desk

By deciding to outsource these functions, XYZ realized significant cost savings in both up-front (one-time) costs and annual recurring costs. It is estimated that up-front startup costs would have been ***200%*** greater and annual recurring costs would be ***800%*** greater had XYZ decided to manage these functions internally with their own personnel.

In addition to significant cost savings, the operational efficiency and effectiveness of the XYZ's physical and electronic security program has benefited considerably. This case study studies the factors leading to XYZ's decision to outsource to SSC.

Problem Statement

Shortly after September 11, 2001, one of the world's largest bottler of beverage products (referred to as 'XYZ Company' for the purpose of anonymity in this document) – a Fortune 200 company – began re-evaluating the state of security at each of their 47 production facilities in the US and Canada. The objective of the review was to ensure XYZ's employees, assets and production processes were not unreasonably vulnerable to various forms of criminal activity.

The risk and vulnerability assessments led XYZ to immediately implement an integrated enterprise-wide access control system throughout their facilities in the US and Canada. To ensure uniform and consistent security across all of their facilities, they also put in place operational and technical standards for other security measures, such as color-coded photo ID badges, closed circuit television (CCTV) systems and intrusion detection systems.

Management, administration and service of these systems – particularly the enterprise access control system – are considerable tasks, and quickly became key areas of concern for XYZ during the initial planning phases. To ensure their significant financial investment was properly protected, they determined that a dedicated staff of people must be put in place to oversee the security systems' operations.

A decision whether to outsource this function or utilize internal XYZ resources had to be made. Factors affecting this decision were cost, availability of technical expertise, and service reliability. XYZ ultimately decided to outsource, and this paper analyzes the financial and operational justifications of the decision. To protect the integrity of our client, detailed figures and pricing information have been omitted.

Operational Description

The XYZ Plant/Warehouse Security Center (PWSC), managed by SSC (a division of the Aegis Protection Group), has been in official operation since April 1, 2003. The purpose of the PWSC is to perform the following tasks for XYZ:

- ☐ Enterprise Access Control System Administration
- ☐ Centralized Photo ID Badging
- ☐ Service Management and Administration
- ☐ 24x7 Emergency Support and Help Desk

Enterprise Access Control System Administration

The current XYZ enterprise electronic access control system has approximately 1,300 card readers, 40,000 users and 200 intelligent panels in 67 facilities in the United States and Canada. XYZ plans to integrate the approximately 260 remaining facilities into the system over the next 3-5 years.

SSC dedicates personnel to handle all administrative functions of the enterprise access control system. XYZ has assigned local system administrators, but their role is limited in nature, primarily dedicated to requesting badges and assigning access levels to individual cardholders. The full set of administrative tasks required to ensure proper functionality of the access control system includes:

- System programming
  - End points and equipment functions
  - Personnel access level definition
  - Report creation and generation
- Event report review and trend analysis
- Head-end system troubleshooting
- Head-end system maintenance and testing (coordinated with XYZ's IT department)
- End user account management
- Access control system software "Help Desk" for end users
- End user system training and support
- Creation of system-level policies and procedures
- Critical alarm review and response (if necessary)

Should XYZ decide to manage all of these tasks internally (insource), the following steps related to access control system administration must be undertaken:

- XYZ would have to contract with an integration company to provide programming expertise for the GE Picture Perfect enterprise access control system software. Programming is required any time a change or addition is made to the system, including adding or moving a card reader, constructing a new facility, purchasing a new company, or any type of system configuration changes (i.e. access privileges), and requires significant technical expertise.

- The integration company would have to train XYZ's local system administrators how to use the local functions of the system software. Operation of the software again requires technical expertise, and regular turnover in the administrative role could lead to untrained personnel or high costs associated with constant training.

- XYZ system administrators would be solely responsible for regular administrative functions, including running and analyzing regular history and event reports, identifying irregular alarms, invalid cards and

other problems. Depending on the type of report being run, personnel at every facility may dedicate 5% - 25% of their overall job responsibilities simply analyzing reports and purging cardholder databases.

- XYZ would have to contract with an integration company for a system "help desk". The PWSC help desk provides support to all local system administrators for the access control system equipment and Picture Perfect software.

  The PWSC averages approximately 750 telephone calls and 1200 emails each month for support-related issues, such as questions related to the access control system software, maintenance requests and others. It is anticipated that call volume will increase slightly as the system ages, administrators turn over and equipment begins malfunctioning due to the harsh manufacturing/warehouse environment in which it is installed.

- XYZ personnel would be responsible for managing all user accounts. Although this function adds little tangible financial impact to this analysis, it is important to note that this could represent potential security and operational risks if accounts are not managed properly.

Central Badging

The PWSC currently maintains a website that XYZ employees use to request new or replacement photo ID badges / access cards and their related accessories (lanyards, badge holders and retractable clips). Moving from this central badging operation to a system maintained by each facility would be quite costly to XYZ. Every facility must be equipped to supply photo ID badges for their employees, and this expensive equipment must be maintained and regularly serviced. Local personnel would be tasked with operating, maintaining and administering this equipment, which would consume considerable time and require specialize technical expertise.

Other issues that have little tangible financial impact – but could pose significant security vulnerabilities – would come into play should XYZ decide to utilize a decentralized badging scheme:

- Lack of partitioning. The current system does not allow partitioning of the badge database, meaning sites would have the ability to create badges for other facilities.

- Badge design control. The sites would have the ability to change the badge design, potentially resulting in inconsistent ID badges at every facility.

- Double entry errors. Because of the partitioning issue, each site would have to maintain a separate system for badging, meaning every employee would have to be hand-entered into the system to create the badge. Currently this is done through a link with the HR system and the PWSC.

Service Management and Administration

All matters related to service and support of the physical and electronic security systems are initially handled by SSC. A dedicated toll-free number is provided to report any issue or problem. SSC personnel review the issue, perform an initial diagnosis, and then take necessary step(s) to ensure the matter is resolved. If the issue cannot be resolved directly by SSC, the appropriate contractor/company is dispatched to correct the problem. SSC monitors all service calls that are routed to third party contractors to ensure the matter is handled per the contract agreement XYZ has in place with that particular company.

SSC reviews every contract, work item and bill to ensure all payments to the integration companies are made in accordance with contract terms. Any billed item that should be covered under warranty is rejected before

ever reaching XYZ (this is referred to as “warranty enforcement”). Should XYZ decide to manage this function internally, all XYZ personnel that interface with the integration company would have to become familiar with all contract provisions – including national pricing agreements – to ensure XYZ is not unfairly billed.

It has been calculated that SSC saved XYZ approximately $100,000 in the period dating 8/2004 through 8/2005 for items related to warranty enforcement. Assuming SSC did not provide this function for XYZ, this cost savings would not have been realized.

24x7 Emergency Support and Help Desk

SSC maintains a 24-hour help line in the event of a critical system failure, the need for immediate access privilege revocation (i.e. for a terminated night-shift employee that the manager is concerned may become disgruntled), or other system emergency, and commits to responding to the problem within 15 minutes. On-call system administrators have access to the systems from any location, and can usually resolve the issue immediately.

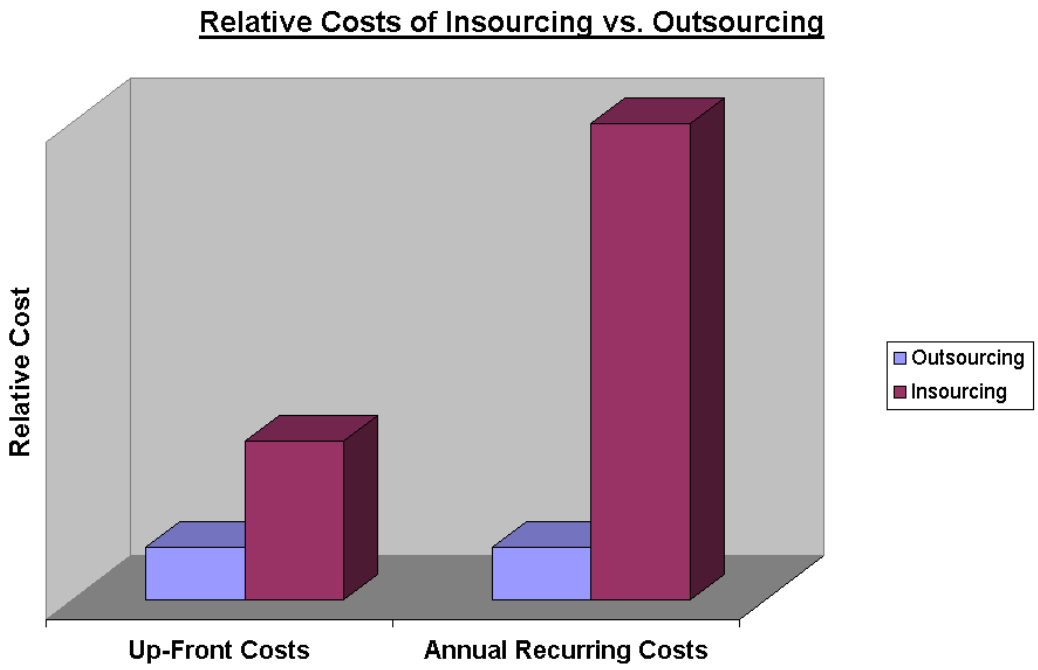
These same trained administrators staff a help desk during normal business hours to answer questions on the operation of the systems, whether related to the software, hardware, website or any other functions. XYZ employees call the toll-free number and have direct access to skilled personnel.

Summary

Outsourcing the security system support services has resulted in operational efficiencies and significant cost savings to XYZ, in both up-front capital expenditures and recurring annual operating expenses. Due to contractual agreements with XYZ, we cannot divulge actual cost figures as part of this report. However, below is a relative summary of the cost savings realized by outsourcing these functions.

When considering whether or not to outsource, XYZ calculated the up-front (one-time) costs associated with implementing the enterprise access control system and photo ID badge program would be nearly ***200%*** higher than outsourcing them to SSC.

Furthermore, the annual recurring costs associated with the proper ongoing operation, administration and maintenance of all electronic security systems would be nearly ***800%*** greater than the cost of outsourcing them to SSC (see chart below).



In addition to significant cost savings, XYZ realized that outsourcing would result in considerable improvements in operational efficiency, and would virtually eliminate the burden of managing and operating a complex physical and electronic security program, while continuing to realize the benefits of such an operation. XYZ decided to protect the integrity of their brand by implementing effective security measures and maintaining fiscal responsibility.