Total Cost of Ownership (TCO) for Access Control Systems

The Importance of Considering All Costs When Comparing the Initial Costs of Access Control Systems.

An RS2 Technologies White Paper

400 Fisher Street, Suite G
Munster, IN 46321
www.rs2tech.com

Total Cost of Ownership (TCO) for Access Control Systems

The Importance of Considering All Costs When Comparing the Initial Costs of Access Control Systems.

Table of Contents

©2008, RS2 Technologies, LLC. All rights reserved. RS2, RS2 Technologies, Access It!®, and the RS2 logo are all trademarks of RS2 Technologies, LLC. All other trademarks are the property of their respective owners. Information contained within this document is intended for general educational purposes and is subject to change without notice. It is considered to be accurate at the time of publication, but RS2 Technologies, LLC assumes no liability and makes no warranties, express or implied, with respect to the accuracy of the information or its use for any purpose.

Executive Summary

The actual cost of owning and operating an integrated Access Control System involves a combination of costs that go well beyond initial acquisition costs. When evaluating Access Control Systems, end users, System Integrators, dealers, and security consultants would be well advised to look at the entire spectrum of acquisition, operating, upgrade, maintenance, training, travel, and other costs when evaluating Total Cost of Ownership (TCO) of an Access Control System.

This White Paper examines a number of components of the TCO equation, and discusses how the TCO concept can be effectively applied in the decision-making process involving the choice of an Access Control System supplier. This paper does not provide an absolute quantitative model for side-by-side cost comparison of competing Access Control Systems. Rather, it looks at the four major cost components of Access Control System ownership and provides a list of questions that decision-makers should ask potential vendors. The reader is then encouraged to apply the TCO concept to his/her next Access Control System purchase decision.

Possibly the largest part of Access Control System ownership cost actually lies in ongoing costs, not initial hardware & software costs.

What is Total Cost of Ownership (TCO)?

What is TCO? Total Cost of Ownership (sometimes referred to as Total Life Cycle Cost) is, as the name suggests, simply a way for purchasers and specifiers of Access Control Systems to understand, evaluate, and ultimately manage **all** the costs involved in their purchase, including up-front costs and after-purchase costs (both direct and indirect). TCO is not rocket science. A very contemporary analogy would be the purchase of an automobile. The TCO of automotive ownership doesn't end with an attractive, rebate-enhanced purchase price. Gasoline, maintenance, non-warranty and post-warranty repair costs, and insurance premiums figure into the automotive TCO equation. And, while similar to the automotive analogy, TCO for Access Control Systems is even more complex, as it must include factors such as system performance and reliability.

Until relatively recently, Access Control System buyers commonly thought of system costs in terms of the up-front hardware and software expenses associated with IT systems or sophisticated electronic office equipment. However, experience has shown that possibly the largest part of Access Control System ownership cost actually lies in ongoing operational expenses, maintenance, and support agreements, because Access Control Systems must be held to a much higher standard of availability and performance than office equipment or even general-purpose IT systems. The costs of Access Control System downtime, lost productivity, and business risk cost of system unavailability, while tangible (and even sometimes catastrophic) can be difficult to quantify and are, therefore, not examined in detail in this paper.

Access Control System Cost Components

This section examines the four major cost components of Access Control Systems, which are:

- Hardware Costs
- Software Costs
- Support Costs
- "Hidden" Costs

Hardware Costs

With open architecture systems, end users are not tied to the products of a specific manufacturer.

With some exceptions, this first cost component, hardware, is the most easily definable cost in the Access Control System TCO equation, particularly for brand new installations. In such cases, purchase decision-makers can prepare lists of the system control processors, readers, I/O modules and other peripherals that they will need to complete their system. In the case of retrofit installations that can make use of some –or all– of the existing hardware, the process is similar but the equipment list is shorter and the investment in hardware is lower.

At this juncture, a few words about the benefits of "open architecture" Access Control Systems is appropriate.

The Value of Open Architecture

The question of "open" versus "closed" systems (sometimes referred to as "standard" versus "proprietary") has been debated for years in the access control industry, but, generally, most experts have now come out in favor of the open architecture concept. (This subject will be treated in greater detail in a future RS2 White Paper.) Stated as succinctly as possible, open architecture systems use widely available hardware platforms that allow end users to utilize equipment from different Access Control System manufacturers. The advantages are numerous, with the most obvious being that end users are not tied to the products of a specific manufacturer. This allows them to add features provided by new technology that might be offered by a different manufacturer than the vendor from whom the initial system was purchased. This assumes, of course, that their **original** installation is based on an open architecture system.

While there are several manufacturers of open architecture access control hardware, the largest manufacturer in the U.S. is Mercury Security Corporation. RS2 Technologies works exclusively with Mercury. In the past, we also worked with other hardware manufacturers, but we have found that Mercury hardware allows us to offer the most features to our customers – at the best price. It is also important for specifiers and end users to be alert to the fact that, while many Access Control System companies use Mercury hardware, not all of them write software that is compatible with all three Mercury platforms. Some companies "code" only to Mercury's older SCP family, while others code only to the second-generation AP family or to the new EP series. RS2 Technologies codes to the SCP, AP, and EP families. (Note: At RS2, we refer to the AP series as the 2g – for 2nd generation.)

Other hardware-related costs can include wiring/cabling and other electrical components, and the actual cost of installation by dealers or System Integrators, plus costs for electricians and other skilled personnel. Similar to the actual Access Control System hardware, these ancillary costs can also be affected by the type of system (open vs. proprietary) chosen. End users should consult with their system integrator to ascertain if this is the case.

Software Costs

Software costs can significantly increase TCO over the life of the Access Control System.

Software costs, while representing only a fraction of **initial** system investment, have significant potential for driving up **ongoing** Access Control System costs and, therefore, TCO. Decision-makers should be extra vigilant when evaluating and comparing software costs. Common software-related cost pitfalls include:

- Reader Licenses
- Software Maintenance Agreements
- Software "Add-Ons"

Many software manufacturers charge for "reader licenses" based on the number of readers supported by their software. Reader license packages will be sold for 32, 64, 128, or 256 (and up) readers. RS2 Technologies does **not** charge for reader licenses, but instead includes support for several different levels of readers in both its standard and enterprise-level software packages. I.e., reader support is already included in the base price of the software.

"Software Maintenance Agreements" can significantly increase TCO over the life of the Access Control System. They vary from manufacturer to manufacturer, but the basic premise is that software manufacturers will charge dealers and/or end users ongoing fees for routine support over the life of the agreement. RS2 Technologies does **not** have Software Maintenance Agreements. Instead, RS2 will assist any authorized RS2 dealer in good standing – **at no charge** – in supporting any customer who is using a "supported version" of any RS2 software package, whether or not they are on the most current version. And, to help customers cost-effectively upgrade their software, RS2 offers a Version Upgrade (VU) program. As a customer's system grows, the VU program allows them to move up from one software level to the next and receive **full credit** for their previous investment. This reduces customer costs in two ways. First, it allows RS2 System Integrators to quote the **minimum** – and therefore least costly – level of software necessary to accomplish the immediate project objectives. Then, when system needs grow to the level where a software upgrade is required, the RS2 VU program protects the customer's initial investment by giving full credit for its cost against the cost of the upgraded software.

"Add-ons" can be another potentially costly misstep in the software minefield. Many Access Control System software manufacturers charge extra for features such as form design and map design. These and several other features are standard in RS2's software. Purchasers should have a clear understanding of what is –and is not – included in every software package that they are considering. (See "Questions to Ask Access Control System Vendors" on page 10.)

Support Costs

Support costs can account for up to 65% of ACS TCO over the life of the system.

Some studies suggest that support costs can account for up to 65-70% of Access Control System TCO over the life of the system. Therefore, identifying and controlling support costs can be as important –or more so– than controlling hardware and software costs. While support costs can include any number of elements, for the purpose of this White Paper, we will concentrate on just two items:

- Training Costs
- Help Desk/Troubleshooting Costs

Training Costs

Training costs include both initial and ongoing training, so the cost of initial training is often included under "installation" or "start-up." However they are classified, training costs can be significant. Many Access Control System vendors charge for initial training and most charge for ongoing training. Moreover, they require that training be done at their (i.e., the vendor's) facility, so end users also incur the high (and getting higher by the month) costs of travel. Added to this is the cost of pulling employees away from their regular jobs to attend training sessions. While it is true that, even if the Access Control System vendor will conduct all training (initial and ongoing) at the customer's location, there will be a certain amount of "time off" for training, but this time investment is increased greatly if those employees must travel to the training site.

RS2 Technologies does not charge for any training – either of dealers or end users. Moreover, RS2 assumes the burden of travel costs and time investment by traveling to dealer and/or customer sites to conduct initial and ongoing technical training and certification. This reduces personnel "downtime" for training.

Help Desk / Troubleshooting Costs

While some Access Control System manufacturers do not specifically charge for access to their Help or Support/Troubleshooting line, many cover this cost by including it as part of their Software Maintenance Agreements (see page 5). RS2 Technologies does not charge customers for access to their Help line and does not have Software Maintenance Agreements.

"Hidden" Costs

As with support costs, any number of items could qualify as "hidden" costs. An example is the hidden cost of unscheduled Access Control System downtime. However, unlike the costs of hardware, software, or support, the costs of downtime can be hard to measure because they can vary considerably from organization to organization, depending on the organization's size, business or mission, and other factors. For example, the costs of system downtime in a commercial business might be measured in lost revenues, reduced employee productivity, or even loss of trade secrets. However, at an educational institution, they might be measured in terms of potentially compromised student safety and the resultant student and parent uncertainty about the institution's ability to ensure same.[1]

Customers should make sure that they can cost-effectively build totally integrated Access Control Systems.

One hidden cost that is common to many systems, regardless of mission –and one that can be measured in dollars– is the cost of integration with other Access Control System elements. To begin with, the Access Control System must be able to integrate with a number of devices. Typical examples would be:

- Digital Video Reorders (DVRs) and/or Network Video Recorders (NVRs)
- Closed Circuit Television (CCTV)
- Intercom Systems
- Intrusion Detection Systems

Access Control System manufacturers who are unable (or, in some cases, unwilling) to integrate with the products of other security device manufacturers simply raise TCO for their customers. In the past, Access Control Systems and other security devices such as intrusion detection systems were installed using separate cabling, door contacts, etc., which increased system installation costs. Also, the systems typically did not share data, making it difficult to associate various alarm and access control events. Today, manufacturers such as RS2 Technologies integrate their software with a number of manufacturers of such products. (RS2 has more than 15 integration partners for devices and an equal number of strategic partners for products and services such as Visitor Management.)

A number of Access Control System manufacturers have their own lines of security products such as DVRs and either will not integrate with other manufacturers or will make the process very difficult. RS2 does not manufacture any DVRs, NVRs, CCTV cameras, intercoms, or intrusion detection systems and will integrate with almost any manufacturer of these devices/systems. Access Control System specifiers also need to be alert to how manufacturers charge for integration with various devices. For example, when integrating with DVRs and cameras, **some manufacturers will charge customers for every single DVR and camera that is attached to the system.** RS2 Technologies charges only by the **client seat, not for each DVR or camera.** For example, a system in which two guard desks and one administrator need to see camera views simultaneously would have three "client seats."

[1] Read about how the University of Pittsburgh successfully used their RS2 Technologies Access Control System to control multiple campus functions by calling 877.682.3532 and asking for a copy of the July, 2007 *Security Management* article "Campus Access Controlled".

Customers also need to get a full list of integration features from the Access Control System vendors they are evaluating. This will ensure that they can cost-effectively build totally integrated systems in which all the elements communicate on the same network and which can be controlled from a single, consistent graphical interface. The issue of Access Control System integration is so important that RS2 Technologies will treat it in a separate White Paper in the coming months.

Adding Up the Costs

A 3-year comparison showed significantly different TCOs for three similar systems.

In Figure 1 (below), costs were compared for a typical multi-door Access Control System installed in a large office building, in which the system was integrated with a video surveillance system, CCTV, and several intercom stations. In addition to initial procurement and installation costs, the first three years of costs for training, software maintenance agreements and integration fees were included. As illustrated by the graph, while hardware costs were similar for all three systems, significant differences were found in training costs and ongoing costs. The costs of downtime and system unavailability were not included in this comparison.

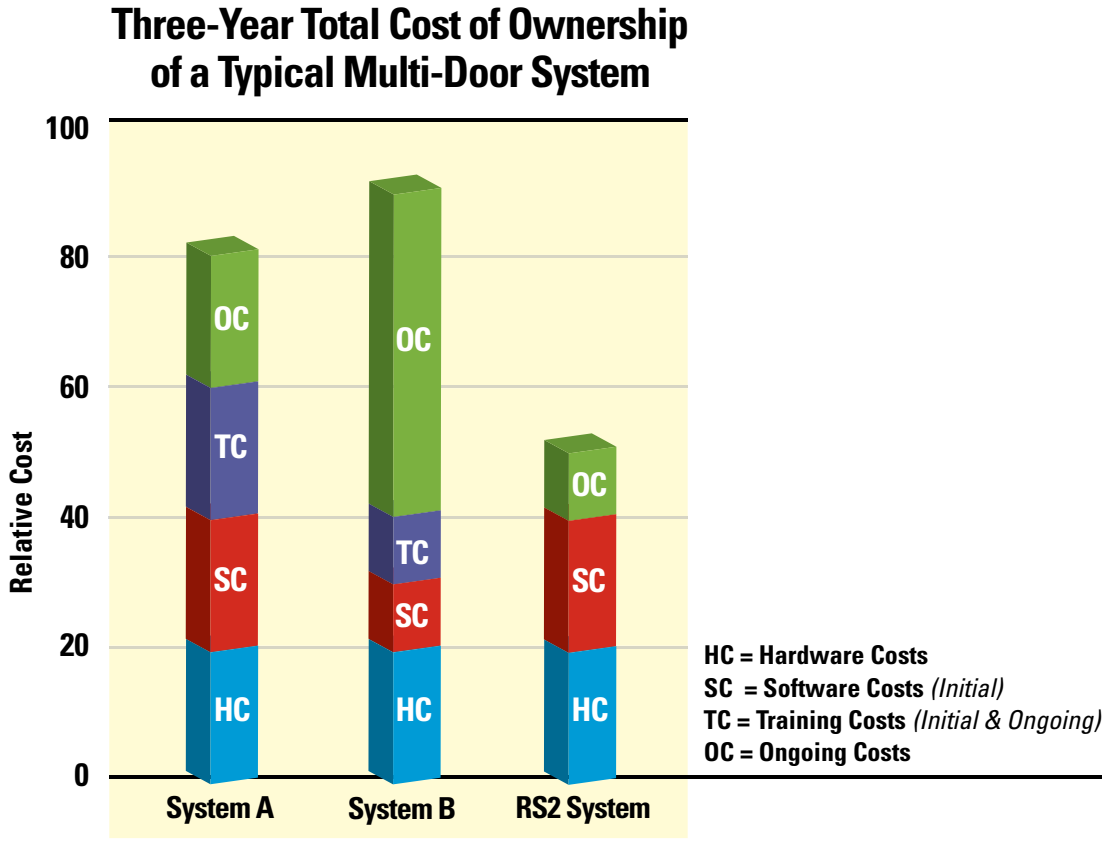

Figure 1: In this example, Ongoing Costs included reader licenses, ongoing training costs, software maintenance agreements, version upgrades, patches/fixes, and staff travel costs for training.

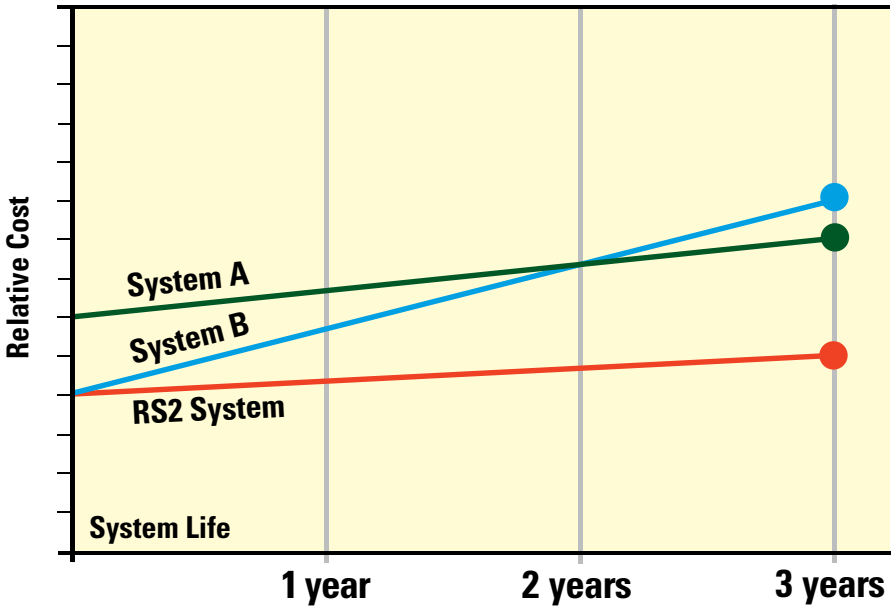

Figure 2: Cumulative TCO over 3 years.

Another useful view of the same data is shown in Figure 2, in which costs are shown over the first three years of system operation. This graph illustrates how, while the original investment in hardware, software, and initial training for System B and the RS2 Technologies system is roughly equal (with System B somewhat less than System A), the significantly higher ongoing costs for System B result in a cumulative TCO that is approximately 12% higher than that of System A, and almost 80% higher than that of the RS2 system.

Other Factors

This White Paper has already discussed some of the factors that are not easily quantifiable, such as system downtime and integration of the system with other security devices. Even more difficult to quantify in dollars, but equally as important as any factor already discussed are such items as:

- Hardware reliability
- Software ease-of-use (i.e., user friendliness)
- Flexibility and responsiveness of the Access Control System manufacturer

Access Control System purchasers and decision-makers can research hardware reliability by consulting various published security industry sources (both print and Internet). As previously stated, RS2 Technologies and other manufacturers use the highly reliable, industry-standard hardware produced by Mercury Security Corporation.

Software ease-of-use is best evaluated by actually running software demos, by contacting other end-users who are already running the system, and by talking to dealers and System Integrators. The latter two avenues would also be the best

means to ascertain which Access Control System manufacturers are responsive to their dealers, System Integrators, and end-users, as well as to industry changes and customer demand for new features. While these might seem to be "soft" criteria when computing ACS TCO, many companies have found that they have ignored them at their peril. Horror stories abound of end-users saddled with software so difficult to use that they have had to assign "shadow" staff to support it.

Questions to Ask Vendors

So, what are some of the questions that purchasers of Access Control Systems should ask vendors? A partial list would include:

Decision-makers should not hesitate to "hold vendors' feet to the fire."

- Does your system use "open architecture" hardware?
- If so, who is the manufacturer?
- Is your software written to support all generations of this manufacturer's hardware?
- What is your policy on reader licenses?
- Do you require customers to sign Software Maintenance Agreements?
- Do you have a Version Upgrade program? How does it work?
- What is – and is not – included in the base price of your software?
- Do you charge for initial training?
- Where is this training conducted?
- Do you charge for follow-up training?
- Where is this training conducted?
- Do you charge for access to your Help line?
- Will your system integrate with other security devices such as DVRs, CCTV, intercoms, etc.?
- What is your schedule of charges for integrating with these devices/systems?
- Do you charge by the "client seat" or for every single device (camera, DVR, etc.) that is attached to the system?
- Can you provide a list of end-users who will talk about their experience with your system and your company?

Conclusions

Total Cost of Ownership (TCO) is a price/performance metric that is extremely useful for comparing the costs of competing Access Control Systems because it allows ACS specifiers to evaluate systems based on the total cost to own the solution. It is essential that end-users, dealers, System Integrators, and security consultants use this metric when evaluating competing systems. They should –at a minimum– ask ACS vendors the questions outlined in this White Paper, and they should avail themselves of the expertise of manufacturers of access control hardware and software and of the products (DVRs, NVRs, CCTV, intrusion detection and intercom systems, etc.) with which Access Control Systems are integrated.

When evaluated using TCO, RS2 Technologies Access Control Systems deliver the highest business value in the access control industry.

About RS2 Technologies, LLC

RS2 Technologies, headquartered in Munster, Indiana, is a technology-driven developer and manufacturer of cutting edge access management hardware and software. The company's hardware line includes a wide range of system control processors, input/output modules, multiplexers, card readers and proximity and smart cards. RS2 also offers the industry's most advanced, easy-to-use software with its **Access It!**® line of access control software. RS2 is a Microsoft Certified Partner with ISV (Independent Software Vendor) software solutions competency status.

For more information, visit our web site at www.rs2tech.com or contact:

RS2 Technologies, LLC
877.682.3532
inquiry@rs2tech.com