August 2012

SECURITY

SOLUTIONS FOR ENTERPRISE SECURITY LEADERS

Most Influential People IN SECURITY

FEATURING

DOROTHY BITNER, GREGORY BUJAC, MIKI CALERO, STEVEN R. CHABINSKY, *DOMINIC CROWLEY, CLARK KENT ERVIN, RICHARD GRASSIE, JOHN HAMRE,* JAY HAUHN, MITCH LAWRENCE, GRANT LECKY, TIM MCATEE, *TIMOTHY J. MCQUIGGAN, JANA MONROE, RONALD NOBLE, JOHN O'CONNOR,* JOSEPH PETRO, LAURIE SCHIVE, JOHN SMITH, JAMES F. SNYDER, *JOHN STEWART, HOWARD TIMM*

A bnp media Publication

A Deal You Can't Refuse:
Access Control on a Tight Budget

By Claire Meyer, Associate Editor

The problem is ageless – you want outstanding security to protect your organization's assets, but where does the money come from? CSOs across the globe have to petition their CFOs and other C-suite executives for appropriate funding to meet compliance requirements, keep software up to date and, generally, keep the right doors closed.

When Keystone Biofuels upgraded to a new location, it had to find a way to protect its multi-million dollar facility and the hundreds of thousands of gallons of fuel it contained.

So riddle me this: If budgets are tight and pocketbooks are closed, how do you keep card readers functioning and facilities locked down?

For many, the key is in not necessarily what you buy, but how you buy it.

Depending on your vendor or integrator, you might be able to cut a deal by either working out a payment plan or installing an access control system one door at a time.

Keystone Biofuels in Camp Hill, Penn., was looking for the bare-bones security system. The company had recently moved from their old plant – a rented rail shed where the only form of access control was a pull-down door and a lock – to a larger facility with rail access and several million dollars worth of brand new equipment, fuel and stock.

But, by the time Keystone Biofuels was finished building its facility, it was time to consider security, and at that point, there was the problem of cash flow.

"We told our vendors what we could afford and what we were looking at, which was the absolute minimum we could do in terms of security," says Denise Lewis, the executive administrative assistant of Keystone Biofuels, and the ad-hoc security monitor in the company of 19 employees. "M3T, our integrator now, is the one that came back and said 'For the value of the assets you're trying to protect, maybe you should consider a 36-month payment plan.'"

It's essentially an ongoing security-as-a-service plan – Keystone gets four HD cameras and proximity card readers from RedCloud on each of five doors. All of the access logs and surveillance footage is stored offsite and monitored 24/7, which in a company of 19, "is definitely the selling point," Lewis says.

Keystone pays M3T to print their access control cards, which can be reprogrammed for new users to save on costs. The card readers provide entry analytics and auto-lock capabilities, and the cameras are positioned outside and inside the plant to verify alarms and detect any unwanted behavior.

According to Mark Clarke at M3T, a comparable system's hardware and installation alone would cost an end user upwards of $20,000. Keystone Biofuels pays less than $1,000 a month, including the monitoring costs, installation, training and a warrantee, with no up-front cost.

But small companies are not the only ones keeping a close eye on their pocketbooks. CoorsTek, a manufacturer of technical ceramics, has facilities in North America, Europe, South America and the Pacific Rim, but each facility has been left primarily to its own devices in terms of security, partly because of their incredibly diverse locales. Through occasional acquisitions through the years, CoorsTek facilities were operating under equally diverse access control systems, using client-server systems and lots of bandwidth, and many were too expensive to maintain and couldn't integrate with other systems. So when Scott Weisgerber, CoorsTek's Regional IT Manager, was looking for more unified accountability from the buildings, he started to investigate solutions that could be implemented bit by bit.

"The individual facilities maintain their own budgets, their own time schedules for integration," Weisgerber says. "We don't roll out a complete plan for door security. Coming down to the local plant manager, they want to be able to budget that in. With Infinias and Intelli-M, they can do it one door at a time."

That one door, including hardware and the installation, costs just less than $1,000. If the controller or reader is the only hardware update required, the price drops to a mere $300.

"In most cases, we are able to use the existing prox readers and the locking mechanisms, so it's pretty easy to fit a few doors into your retrofit facility," he adds. "A lot of your time and labor is in the locking mechanism, so by reusing those, you can save a lot."

By using Power over Ethernet (PoE), the solution requires less wiring and installation costs, and the project gradually integrates all of the sites into one global system.

Access records through the system are centralized for the entire company, giving the corporate side of CoorsTek more accountability for their branches.

Also, when an employee leaves the company, CoorsTek only has to remove one record and security clearance is removed for all facilities.

However, one day, if the stars align in just

Tallying Up Your Total Cost of Ownership

Even though the proposed cost of your new access control system has you breathing a sigh of relief, don't sign that agreement quite yet. You still have quite a bit of math to do.

Although the hardware in your access control system is often the biggest chunk of the cost, there are other factors to consider when calculating the system's Total Cost of Ownership (TCO). The four major components to consider are:

Hardware Costs

According to a recent whitepaper from RS2 Technologies, hardware might be the most easily definable expense, but it's important to remember to calculate in the costs of wiring or cabling, electrical components, the cost of installation and the payment of any electricians or personnel working on the project.

Software Costs

Software costs might represent a mere fraction of the original system investment, but ongoing charges really add up in this component. Common pitfalls are found in reader licenses, software maintenance agreements and software "add-ons."

Some manufacturers might charge based on the number of users per reader license, which can change costs as an organization expands. Software maintenance agreements are often packaged as a "security as a service," with ongoing costs over the life of the agreement. These services can be quite useful, if not necessary, but it's important to leave room for it in your access control budget.

"Add-ons" can be especially pricy, especially if you decide to supersize your security system. Certain features, such as form and map design, are often an extra cost.

Support Costs

Some studies suggest that support costs can account for up to 65 or 70 percent of an access control system's TCO – the most calculable figures include training costs and help desk or troubleshooting costs.

Training costs include both initial and ongoing training, and vendors might require that training be held at their facilities, requiring travel expenses in addition to a loss of productivity as workers are pulled from their usual posts for off-site lessons.

Troubleshooting and help desk services can be either complementary or paid options in your system, and many vendors cover it under their software maintenance agreements.

"Hidden" Costs

These costs, while very real, are often difficult to calculate – such as the cost of system downtime – or entirely dependent on the size or nature of an organization. One certain expense that every security director should look at with a sharp eye is the cost of integration with existing access control elements, such as DVRs or NVRs, the security surveillance system, intercom systems and intrusion detection systems, according to the RS2 whitepaper.

Other significant factors that are even more difficult to calculate include hardware reliability, ease-of-use and the flexibility and responsiveness of the manufacturer and integrator. By running software demos and contacting other end-users already working with the system, you can get a better picture of how the system would fit into your organization.

the right way, you might find the absolutely perfect solution to your problem at a practical, optimal price.

Jim Govro, director of Facilities Management for Charter Communications, is certainly thanking his lucky stars for his teamwork with access control provider RS2.

Charter Communications has more than 4,600 locations and needed a non-proprietary card access system that reused as much equipment as possible. Charter adds approximately 100 locations every year, between retail, customer service, manufacturing and offices. Out of those, 60 are retrofits.

With such a sprawling enterprise, Govro has to keep costs down. So instead of calling an integrator for every error message, RS2 trained a team of Charter employees to troubleshoot the access control panels, which cost $700 to $1,000 each.

"Even though it's a low cost product, it's a very high security value," Govro says. "You don't have to spend hundreds of thousands of dollars when you can spend $10,000 and get the same effect. For us, it works. If I just want to do one door, I can, and I can do it a couple different ways without spending too much."

Access control systems can also give back to the company to improve ROI and reduce risk, even on a dime.

At Charter Communications, access control isn't only cost-effective, it prevents loss at manufacturing and customer service facilities nationwide.

Govro's system features an auto-dial or email alert program that, when there's an equipment failure at one of the facilities, sends a notification to the repair company so the technician can arrive on the scene and start repairing the damage faster.

The new system also slowed shrinkage at warehouse and distributing centers for Charter, as an automatic email is sent to the facility manager when a door is keyed open at 2 a.m., for example. The email arrives with the employee's name and phone number, so the manager can call the person directly and inquire why they decided to take a late-night stroll to work.

"That gives us the best ROI – just knowing what's going on onsite, and having a report on hand in a matter of minutes," Govro says.

At CoorsTek, also, the access control program is working double-time to improve conditions in factory settings, as it helps to keep a running record of who is checking possibly toxic waste water.

"We had a waste water station, where things had to be tested before it's drained," Weisgerber says. "We added the controls so it couldn't be drained without someone keying in that it had been tested for pH levels."

Added uses add value, which helps to offset your, albeit modest, investment in the latest access control, and adds to your department's reputation as a problem solver, not just a cost center.

So when evaluating what kind of new access control you can fit into your budget, don't settle for the bare-bones solution. Instead, start asking your vendor and integrator if they can make you a deal you just can't refuse. SECURITY

Multi-Technology Readers Let You Pick the Pace of Migration to More Secure Smart Cards

By Jeremy Earles, Portfolio Manager, Credentials & Readers, Ingersoll Rand Security Technologies

While 125 kHz proximity technology is the common technology in today's access control systems, 13.56 MHz smart card technology is the technology of tomorrow because it provides more security and storage for access control systems. Additionally, today, the cost of a smart card is comparable to that of the standard, traditional proximity card, which is the most used card in physical access control today.


Jeremy Earles

Yet, it provides much higher security than a proximity card along with the ability to handle a wide variety of applications from holding biometric templates to being used for cashless vending. Thus, the comparable cost alone removes a major impediment to the use of smart cards. It is very important that all organizations be prepared for smart credential deployment, even if that facility wants to install proximity at present.

Multi-credential readers are perfect for these locales. Besides aiding implementation, multi-technology readers are available to create flexibility in the transition while allowing your organization to leverage the lower cost of smart cards.

With a multi-credential reader being installed at every new door, you are able to flexibly plan for the future. Since multi-technology readers work on both the proximity frequency and the smart card frequency, you can still use your current proximity credentials while migrating to smart credentials at your own pace.

During the transition, you can use both your old credential and the new smart credential. You can upgrade on your preferred timelines, not due to the whim of technology that forces a "now or never" alternative. When your switch to smart cards comes about, you will not have to tear out and re-install all of your facilities' readers.

NFC-Enabled

Near Field Communications (NFC) technology is now being added to a growing number of mobile handsets to enable access control as well as many other applications. More than 40 million phones are expected to be NFC-enabled by the end of 2012 and over half the phones sold in 2015 will be NFC-capable. In some cases, existing 13.56 MHz smart card/multi-technology readers are already compatible with the new NFC technology which allows your users to use their own smartphones as their credential to enable secure access into their facilities. NFC is one of the key technologies on the horizon.

Using NFC-enabled smartphones in conjunction with your present smart card/multi-technology readers lets organizations be assured that their systems are flexible and their investments are solid far into the future. When NFC-enabled phones are available, you won't have to replace your present smartcard/multi-technology readers. For transition and planning for future expansion, spanning the various technologies of the past, present and future with a multi-technology reader only makes sense in this fast-paced world.