Real Time Networks

The Pieces of ROI

A Framework for Understanding Key and Asset Management Investments

There are many levels of key and asset management and security. A car dealership requires one level of key security while a penitentiary requires another altogether. Some are simple: you put your keys in your purse or your pocket. Some are very complex. Each key or other asset must be signed out and returned under supervision, and authentication is rigid each time that happens.

Providing security for keys and other physical asset costs money—money to hire the people and to define and execute the processes they carry out; money to handle mistakes and crises; money to avoid potential legal and financial exposure should those crises occur. As an organization's key management needs grow, the need to automate some or all of the process grows along with it. At a certain point, manual key management takes too long, costs too much, and is too prone to human error. And this can be true regardless of the size of the organization: a lost key can expose even a small company to lawsuits, regulatory penalties and more.

Just as there are many levels of key and asset management, there are many levels of key and asset management systems, providing many levels of return on the investment. Some offer basic protection only—a locked cabinet connected to a computer. Others offer more advanced functionality—RFID tags that allow automated check in and check out. And some offer full functionality, from check in and out to campus-wide lost key location to automated door monitors stopping people from leaving with protected assets.

You need to find the right tool for the job—one that delivers the right return for the right investment. You don't want to buy functionality you don't need, and when the need is there you don't want to solve it with what amounts to an atomic flyswatter.

There's no template for this; no cookie cutter for determining Return on Investment (ROI). But there can be a framework, a way of breaking down your costs so you can make the right decision about which key management approach you can justify with tangible numbers. That's our goal here: provide that framework, expose some of the core cost points of key and asset management, and offer a guide for you to calculate your own ROI.
We don't know your answers, but we know where to point you to find them.

When you think about ROI, think about how much you'll save on:

- The costs of people.
- The costs of knowledge.
- The costs of error.
- The intangible costs.

The Costs of People

For many, lowering the cost of people is all that's needed to show a satisfying ROI from an asset management system.

Guards

When we say guards, we mean whoever checks keys and assets out and in throughout working hours, monitors exits to ensure assets don't leave the building without authorization, checks to see that fleet vehicles are returned and in good condition, and performs all the other daily, routine manual processes to protect assets.

Fully burdened (benefits, training and so on), the annual cost of a security guard can easily exceed $75,000. If a guard is spending–conservatively–three hours a day stationed by the cabinet where keys are checked in and out, that's almost a third of a shift each day: closing in on $22,000 a year to manage keys and other secured physical assets. (As we say that's conservative; in many cases, maybe most, that guard is stationed by the cabinet all day.) Eliminate that cost, reassign that guard to more critical tasks and stations, and even the most expensive system pays for itself almost immediately. (Don't forget that during peak periods there may be a second guard helping, which increases the cost—and accelerates ROI even more.)

Managers and Administration

That security guard logs the ins and outs of each key/asset assigned to each person. Somebody else must look at those logs for reasons ranging from spotting suspicious trends to basic supervision of the guard's work performance. The suggestion isn't that this takes a massive amount of time. It may be just half an hour, twice a week, every week. It adds up (even more so when you consider the time wasted trying to decipher handwriting, or locate a guard across a large and widespread campus). Forty-eight hours is six days a year. If a security supervisor or manager costs $150,000 (burdened) a year, that's $3500 a year.

FRAMEWORK COST EXAMPLE : $25,500 a year for people.

Contact us to schedule an Online Demo:
1.800.331.2882

www.realtimenetworks.com

The Cost of Knowledge

Those reports that managers spend an hour a week reading have a cost of creation associated with them. The depth, granularity and analysis of those reports drives the cost of reporting, as well as the value the reports deliver to the business.

In some cases, a “report” is nothing more than a photocopy of the daily logs. At a higher level of sophistication, the guard may use a spreadsheet for check out and check in and the printout of that is a report. But in neither case is there analysis—no mechanism to quickly slice, dice and drill down through a week’s worth of asset security reports. As key and asset security becomes more important, analysis becomes the critical tool.

Yes, you can get your spreadsheet to run some reasonably sophisticated analyses—if you have a spreadsheet programmer on board or brought in as a consultant. It often works out that the more analyses you perform on your data, the more new analyses you want to add—and that adds up quickly. A full-time spreadsheet programmer, depending on region, can run you (burdened) $175,000 a year. More likely you’ll bring in a consultant, for a week at a time at a rate approaching or exceeding $150/hour. We can estimate that for each new analysis and report you want costs you between $3500 and $6,000. Each. With automated systems, reporting is both included in the basic price, and with the best systems is customizable by users without programming help.

FRAMEWORK COST EXAMPLE :

$6,000 for creating one new analysis/report.

Contact us to schedule an Online Demo:
1.800.331.2882

www.realtimenetworks.com

The Cost of Errors

So far, we've listed the costs incurred if everything goes according to plan. When there are problems, costs skyrocket, sometimes in ways that can't be predicted. The exposure is both financial (the cost of correction) and legal (if the error violates a regulation). Eliminating errors before they happen is core to asset security investment: it's the best insurance you could have.

Forgotten Keys

Sometimes people just forget to return their keys. They walk out the door and don't discover the mistake until they're home. That doesn't seem like a problem. An honest employee just returns the next day and reports the mistake. Still, if at the end of the day a key is not returned, processes and people are triggered to track down the problem, and those processes and people also cost money. There's the cost of alert response, the cost of employee counseling about key responsibility, the cost of reporting the event up the security chain, and other costs. They're individual, small costs, but they add up quickly. Real time alerts provided by an electronic system can help to prevent that key from leaving the building in the first place, eliminating this possibility altogether.

Lost or Stolen Keys/Assets

What are the costs when a key, asset or equipment is lost or stolen? It really doesn't matter which. The same processes are triggered, since it's generally not possible to determine if an item was lost or stolen: you must assume the worst.

The more important that item is, the greater the cost associated with its loss or theft. A key to a broom closet has one set of costs associated with it. A master key to an entire building has a much greater cost associated with it. Sometimes, depending on the level of security required for that building, a loss might involve rekeying the locks on the building and supplying a new set of master keys.

Costs can get huge. A Grand Master Key for the University of Central Arkansas was stolen in 2012. The university paper reported that its cost to replace was $100,000 and involved the direct approval of the Chancellor and the Trustees.

But let's not think of the extreme case. Let's say that it's a regular key that opens 25 doors, and that identical keys are used by 50 people. Those 25 locks must be rekeyed at about $50 a piece. New keys must be made, including master keys for—according to industry averages—about $5 a piece. That means each event costs $1500 in material and labor; now add in the costs of the security staff who have to deal with the loss—report it, log it, investigate it, and enroll and distribute the new keys: another $500.

FRAMEWORK COST EXAMPLE : $2,000 each event.

The Intangible Costs

The Cost of Authentication

What's your exposure if an unauthorized individual gains access to a room, a building, a vehicle or to other assets. What's your exposure if your authentication system breaks down—if, for instance, a PIN is shared or stolen? If that exposure is significant, you'll want to see whether biometric authentication, alone or as part of two-factor authentication, should play a role in your system.

The Cost of Compliance

The compliance burden over key and asset security is minimal for some and overwhelming for others. In many cases, failing to comply with key control policies or regulations around securing firearms, OC Spray cans or police evidence—whether it's failing a log audit, unreported or reported instances of lost items, or keys mistakenly taken from the building—carries serious penalties. One other thing to consider. If those penalties are harsh, an employee that forgets or loses items a couple of times can be fired; in that case you have to add new employee onboarding to the cost of compliance.

The Cost of Disruption

When there's an event with a key, or any other asset, business is disrupted. Disruption ripples and each ripple carries a price tag. You have to find the cost of each ripple.

The people who lost the keys, tools or equipment can't do their job until they're issued new ones. Neither, for that matter, can the people tasked with handling the administration side of the loss: recording, reporting and issuing the new items. They've got better things to do too. And there's the risk that other work is delayed while the problem is dealt with—delays that can infect much of the organization.

Recapping Framework Sample Costs

Let’s go back quickly and do some addition—summing up just those ROI elements that are tangible and leaving the intangible costs (like disruption and non-compliance) as your homework assignment.

$25,500	a year for people.
$6,000	for one new report each year
$2,000	for each lost item.
	Unknown intangible costs

TOTAL : $33,500

Those numbers increase for each new report and each lost/stolen incident over the year.

What’s Right for You

The numbers we used here may not be the right ones for you—but the framework for determining your costs is right. Look to the people, the processes, the reporting, the cost of errors, and other costs as you find them. That’s where you start. Then look at the solutions that are out there, and ask the questions we’ve listed below.

One last word. Real Time Networks is here to help you apply this framework to your business, your real costs, and your tangible and intangible threats and exposures. Contact us to get that conversation started.

Contact us to schedule an Online Demo:
1.800.331.2882

www.realtimenetworks.com

ROI QUESTIONS FOR YOU

- What's the cost of guarding keys?
- If key guarding is eliminated, how much else will you get done with the same staff?
- How much money will you save by automating logging and reporting?
- What does it cost to create a report?
- What does it cost to read a report?
- What does it cost to respond to the information in the report?
- How much money will you save by eliminating spreadsheet reporting?
- How much does it cost to replace a lost key?
- Who has to approve the replacement—and how much does it cost to get that approval?
- How long does it take to get the key replaced?
- How much work is stopped or disrupted until the key is replaced?
- What's the combined costs of disruption when a key is lost or stolen?
- What is the potential exposure to the business of identity theft or PIN sharing to gain access to assets?
- What are the penalties and costs associated with failure to comply with key security policies and regulations?

1 800 331 2882
www.realtimenetworks.com

Real Time Networks

Learn more about key & asset management solutions.

For further purchasing advice, or to learn more about selecting the right Key or Asset Management System for your organization, talk to an expert at 1-800-331-2882 or visit us online at www.realtimenetworks.com.

Since 1989, Real Time Networks has been a leading provider of custom safety and security solutions, including RFID key control systems, electronic asset lockers, and indoor positioning systems for keys, assets, and people. It has earned the reputation of solving complex key and asset security challenges for their customers, and delivering custom security solutions that are backed by industry-leading customer service. Real Time Networks caters to the needs of thousands of clients in: Law Enforcement, Corrections, Gaming, Managing Fleets and Parking, Education, Hotels and Hospitality, Government, Museums, Retail Loss Prevention, Sports, Healthcare, and Air Travel.

From your initial consultation and gap analysis, to custom installation, to on-site training, all the way to toll-free phone support and on-site support, Real Time Networks keeps you and your technology running safe, secure, and efficient.