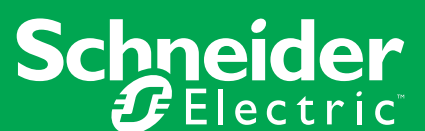


Three levels of Security

Make the most of your energy^{SMThr}



Three levels of Security

To make the process of articulating Return on Security Investment easier, Security professionals looked for new easier ways to make a convincing case for the investments they needed to deliver proper Security Management Solutions. One of the options was viewing Security Management Solutions in categories.^{6, 7} Three categories emerged, with their differences delineated by the scope and impact a solution provides to an organization.

The categories can be outlined as follows:

- 1. Solutions that provide Security Effectiveness
- 2. Solutions that Reduce Risk
- 3. Solutions that deliver Business Efficiency

Each level provides specific benefits to the organization. Those benefits can be mapped to Return on Security Investment. (See Illustration 1.)¹⁵

Value	Customer Benefits	Results
Security Effectiveness	CAPEX and OPEX cost reductions result from integrating multiple disparate technologies onto a single, comprehensive Security network.	€
Risk Reduction	Securing the people and assets that make up a business reduces risk, ensures business continuity, and enhances reputation. Real financial benefits are many.	€
Business Efficiency	The investments customers make in Security technology can be leveraged to improve business processes, reducing variable costs and increasing revenues.	€

Illustration 1 Three Levels of Security

The first level: Security Effectiveness

The promise of Security Effectiveness represents the most basic reason why executives invest in Security Management Solutions. Integrating multiple disparate technologies onto a single comprehensive IT network drives more effective Security Protection. It ultimately results in lower Capital Expenditure (CapEx) costs in new construction and in lower Operating Expenses (OpEx) over time.

This level of Security is exemplified by common and visible systems that are installed in buildings such as cameras, access control solutions and the other tools that might be integrated with these systems (e.g., License Plate Recognition capabilities). These common measures are designed to protect people and assets in an organization.

In enterprise environments, a single system can integrate a Building Management System (BMS) and Security. Such a solution is easier to operate than many disparate systems. Hence, long-term cost containment (lower OpEx) is achieved in several ways:

- Training cycle time is shorter with user-friendly single command and control systems; therefore, training costs decrease;
- Operators are more efficient because they are only managing one control platform versus numerous dashboards; therefore, a smaller number of staff members is necessary to manage the single system;
- Job satisfaction – and hence employee retention – increases because integrated systems are easier to learn and operate.^{6, 7}

In addition to enabling operators to do more with less, Integrated Security Technology enables the provision of additional protection and situational awareness for more square miles or more properties than ever before. In this instance, technology not only allows the same number of people to accomplish more, but also it provides the capability to monitor and protect a much larger corporate environment than was previously possible.^{6, 7}

IP intercom and video solutions enable Security operators to remotely monitor facility access. Operators can effectively interrogate visitors through an intercom system and at the same time, view them using video surveillance. It is not necessary for Security personnel to be posted at each entry point or even situated on-site.

In critical infrastructure environments, different Security systems may be integrated so that many separate law enforcement and Security entities can economically maintain Video Surveillance. Integrating these disparate Security systems onto one common Security Platform also enables sharing of actionable video data between the agencies. This reduces overall costs not only for the agencies themselves, but also for the facility as well. In addition, this strategy delivers highly-effective Security monitoring protection so operators in these critical environments can be extremely responsive and quick to address potential threats.

In globalization efforts in which corporations expand into new territories around the world, Integrated Security Infrastructures enable professionals to ensure that each facility offers a safe environment for operating a business. Integration also makes it easier to manage policies and procedures consistently throughout all the parts of the enterprise.

In a merger or acquisition, two or more companies must rapidly coordinate their respective Security practices and marry their technology infrastructures. The faster the newly-merged company can operate as one entity, the less Business Continuity is impacted. If Security leaders can structure the process and drive the organization toward a speedy outcome, that harmonization can drive not only Business Continuity and sustainability, but also spur more efficient, effective and economical Security Management as well.

Security Management teams must also account for the safety of those who travel or work remotely. Seamless IT and Security access between these workers and their geographically disparate work locations is a critical requirement, something that integration helps accomplish.

Proving the value of all of these Security Effectiveness capabilities has always been a bit problematic. This question illustrates one of the reasons why, “Can a business determine with certainty whether incidents simply did not occur, or conversely, whether the Security Management Solution (and its effectiveness) actually prevented the potential incidents from taking place?” The answer is “no;” therefore, it is difficult for an organization’s management to realistically “prove” that this level of Security investment represents real ROSI. Can executives assign a value to how fast a merger occurs? Likewise, can the monetary impact of having secure mobile workers and travelling staff be assessed? At best, the answer to these queries is “maybe.” In all of these examples, real value is being delivered; however, assigning a fact-based monetary value is difficult.

The second level: Risk Reduction

The second level of value that a Security Management Solution can deliver is Risk Reduction. This level of protection protects brand reputation, bolsters Business Continuity and ultimately provides tangible ROSI.

First, let’s look at some of the major factors that impact Business Continuity: Security incidents, disasters, accidents and non-compliance with regulations. Integrated Security Solutions provide valuable functionality that helps in addressing all of these challenges. A Security solution that provides Risk Reduction gives professionals situational awareness. Having constant awareness of the business environment is a necessary part of anticipating events and providing appropriate responses to potential threats. When anomalies are pinpointed, this kind of solution provides operators with the right information at the right time so that they can make informed decisions.

Disasters such as Acts of God expose valuable assets and people to harm. Security solutions that reduce overall risk allow operators faced with these conditions to manage Security functions remotely if needed. These solutions also provide irrefutable proof of the facts — audit trails — of actual events. Operators can also use Security Management Solutions as a tool to help locate missing assets or people.

Integrated Security Solutions can help alleviate the kinds of interruptions that threaten Business Continuity. Major interruptions in the flow of business come with huge negative financial implications, so in this instance, effective Security ultimately contributes positively to the bottom line.⁷

Now let's consider a few examples in which strategic Security can be used to anticipate vulnerabilities and manage external forces such as regulatory compliance. Due to new government regulations, a global leader in the medical research field faced changes that would disrupt a number of existing processes. With this in mind, management inventoried all of the substances that were subject to the new regulations and designed new Security processes relevant to them. In this case, Security provided protection for the business.

Next, technology was used as an enabling tool to successfully comply with the new regulations. The results were impressive. In a period of 30 months, the team reduced the time needed to respond to a single event by 30%. The number of nuisance alarms decreased by 430%. Both measures helped reduce guard staff costs and at the same time, improved the level of and Security Efficiency in the facility. The organization also reduced its Total Cost of Ownership (TCO) for Security Management. Equally important, administrative costs for generating compliance reports decreased.

Nuclear plants represent another highly-regulated environment. If specific government-mandated regulations are not met, a reactor may be immediately shut down. The government stipulates that a certain number of specifically-skilled workers — SWAT team members, medical personnel, high-level technicians and others — must be on-site in a plant at all times in order to ensure safety and proper operations. Security Management teams play a vital role in compliance by ensuring that access control systems effectively and efficiently monitor and report on the presence of these individuals. Access control systems help to guarantee that a person from one department does not leave the work zone until his or her replacement has arrived.

With this second level of security, the assignment of a monetary value to Security is less problematic. Typically, executives have the background

information to quantify the hourly or daily cost of a business shutdown. They have precedents to gauge financial liability in the event of an accident caused by inadequate protection. Worse yet, they are familiar with the devastating financial effect of monetary settlements levied because proof of what actually transpired was not available. Management also can easily compare the cost of manually gathering the wealth of information needed to prove compliance vs. having the ability to access it automatically. Finally, they know the scope of financial risk associated with non-compliance.⁶

The third level of ROSI: Business value that transcends Security

Using a Security Management Solution to support the primary mission of an organization represents a third level of Security. In this instance, Security technology is used to improve business processes, reduce variable costs and increase revenues.

In this third level, Security is no longer viewed as a technology cost center, but rather, as an enabler that plays a strategic role in an organization. It delivers real tangible benefits in such business areas as logistics, manufacturing, facility scheduling, process improvements and energy management. At this level, Security Management moves from the back office to the front and becomes an essential contributor to overall business success, profitability and continuity. In this realm, executives consider Security as “strategic” and give it a “solutions point-of-view.” This is where Security begins to weave itself into the DNA of an organization.⁷

Let's investigate an environment that relies upon specialization. In this arena, Security professionals can work with the business to deploy technology that supports the skilled labor force. Specialists typically have undergone unique training and certification that extends to such areas as materials handling or working in restricted areas within a facility. In many cases, this type of specialization is regulated by the government or by industry organizations.

Security plays a key role in efficiently managing skilled labor's compliance and the adherence to process. The Security team can help business areas ensure

that the right people are on hand at the right time; that only the appropriate personnel are accessing restricted areas of a facility; and that only specially-designated people are handling certain materials. Laboratories and research institutions provide a great example. In these environments, subject matter experts perform certain roles in which access to sensitive or potentially dangerous areas in facilities is granted based on unique knowledge, expertise and education. Specific credentials – and the Security technology that enables them — are necessary for admittance. In this example, the same technology that protects the business as a whole also enables the specialists in the organization to gain admittance to secured zones and successfully perform the critical functions that generate revenue.

In airports, credentialing plays a key role in securing a facility. For that reason, integrated technology and clearly defined processes are crucially important. On the process side, business rules and work flow are designed to manage the issuance of the credentials required by the access control system. The personnel managing this process must be authenticated by three levels of technology (card, fingerprint, and pin number) before they can be granted the authority to issue credentials to the labor force that will be allowed in secured areas. In this case, Security Management drives safe and effective airport operation.⁷

Another example is a manufacturing environment that employs optical access turnstiles at each assembly line. The turnstiles count staff before production begins for the day and are equipped with a credentialing capability to ensure that only qualified staff members are present and in position. Starting the production line without the proper number of qualified workers may result in a higher propensity of product defects or increase the likelihood of disruptions in the manufacturing process. Using Security technology in this way helps ensure smooth operations.

In a different industrial application, SCADA manufacturing environments, integrating video surveillance and SCADA systems provides significant advantages. One benefit of this scenario is the ability to provide live video

verification of system alarms and events occurring in remote facility locations. In a Water Treatment Plant, for example, an alarm may provide notification that a valve has blown. The data can be confirmed visually before a technician is dispatched to resolve the problem. Visual inspection enables operators to assess the situation and dispatch the right personnel with the right equipment to resolve the issue. Video also helps ensure that individuals are not dispatched to areas exhibiting unsafe conditions. In this example of the use of integrated video and SCADA, the maintenance staff is more efficient and effective than ever before. Staffing is less expensive because the number of facility technicians required to maintain the infrastructure can be decreased. Overall plant operations improve.⁷

Thermal Security cameras provide a great case in point to highlight the benefits of integration. The same thermal cameras used by a Security team to protect a facility can serve the dual purpose of monitoring the temperature of the bearings in pumps and motors. The temperature of bearings increases with excessive wear and thermal cameras can easily detect this change. Operators can then be alerted. Using Security technology to as a preventative maintenance tool helps safeguard against unexpected equipment failure. It also provides a second level of assurance that contributes to Business Continuity – the alleviation of worry that the processes supported by those specific pumps and motors will not be interrupted either. Finally, it means that maintenance staff is proactively dispatched to provide repairs or replacements before equipment failure actually occurs – avoiding an unscheduled shutdown or cascade failure.

Healthcare is an industry in which Integrated Security has revolutionized – and automated — the delivery of customer service by adding effectiveness and efficiency. In hospitals, integration between patient monitoring systems and alarm systems has become prevalent. For example, if a patient's monitoring system triggers an alarm, that alert typically sounds at the nurses' station. The integration of video surveillance technology in patient rooms and nursing stations provides medical staff with an additional decision making and prioritization tool. Not only can nurses hear the patient's concern, but also they can see him or her, thus ensuring the appropriate handling of the alert. Video improves the quality of care, ensures efficient cost-effective nursing and drives higher patient satisfaction.

Another Healthcare example involves integrating a pneumatic tube system with a BMS. In this instance, the pneumatic tube system processes data on-demand in order to allow individual station access control. An authorized individual can employ the "send-secure," "receive secure," and "send stat" elevated access

privileges necessary to retrieve items. The integration is transparent, providing a consistent interface to the system administrator who manages pneumatic tube access control. This pneumatic tube access operates via the BMS user interface in much the same manner as it does for doors and other areas. For over-the-counter (OTC) medications, a user may be allocated low-level access. In the case of morphine or blood samples, however, a much more controlled specific level of access is required. With this kind of system, the hospital can disseminate substances faster and with a higher assurance of safety than ever before. This drives better patient care, more stringent management of controlled substances, lower loss and theft quotients, and less liability for the hospital.

Because of the tie to business processes, this level of Security is easier to assess in terms of ROSI. The capabilities provided by Integrated Security can be shown as tangibly impacting the bottom line.^{11, 12, 13}