The Evolution of Return on Security Investment (ROSI)

January 2012/White Paper

by Kathy Holoman and Aaron Kuzmeskus
Schneider Electric Integrated Security Solutions

Schneider Electric

Summary

Executive summary

The Global Economic Crisis of 2008 had a serious impact on the Security Industry. Although the advanced technology that was nonexistent at the turn of the century had now become plentiful for purchasers, the fragile state of world financial markets made corporate leaders hesitant to actually invest in it. Buyers found themselves with a new pressure – that of justifying Security purchases in terms of Return on Security Investment (ROSI). To make things more difficult, traditional calculations used to measure ROSI were complex and cumbersome due to the many "soft figures" included in them. As executives tried to navigate the new requirement for ROSI, they began to consider viewing Security Management Solutions in three categories, each of which provide incrementally more tangible Return on Investment (ROI):

1. Effective Security
2. Risk Reduction
3. Business Efficiency That Transcends Security

The result was an easier method for articulating the scope of, and the need for, these Security solutions and a clear way to demonstrate ROSI.

A global crisis and its impact on Security

At the same time that the Global Economic Crisis of 2008 loomed on the horizon, the clear divide between Physical Security and Information Technology (IT) began to blur beyond recognition. The roles of Security professionals and IT leaders had become interdependent and intertwined. A frenzy of mergers and acquisitions – and the blending of the information, processes and systems from divergent entities into one made that tie all the more obvious.

The concerns of Security professionals echoed those of IT managers, including the need for scalability, flexibility, and resilience; the desire to meet the wide ranging (and often competing) needs articulated by business silos; the mandate to reduce operating costs; and the requirement to maintain standards and establish clear processes. The evolving climate spurred executive teams to try to plant the seeds of a "Security Culture" by educating employees not only about the need for effective Security Management, but also about the types of value Security might bring to a business.

As global financial markets continued to gain downward momentum, businesses took drastic measures to weather this new storm by making staff cuts, implementing expense controls, freezing capital expenditures and more. This made justifying the purchase of Security Management Solutions even more important. As demand plummeted, Security Integrators saw requests for ways to prove the Return on Security Investment increase incrementally.

Other significant changes were occurring as well. Security regulations that originally were created for governmental entities now were being imposed on private businesses. Organized crime progressively became more sophisticated and more pervasive. Unanticipated threats increased. Reports of workplace violence became more widespread. Natural disasters rocked many regions of the world with a greater frequency than ever before. All of these things drove Security Departments into Risk Management and Business Continuity Leadership, as well as the traditional Asset Protection or Loss Prevention roles.

The emergence of software-driven Security Solutions

By this time, software-based solutions had become prevalent in the new Security landscape. Software-managed Security solutions actually had been one of the drivers for the convergence of Physical Security and Information Technology. Software, data collection & storage, and IT networks all became key elements that enabled the provision of actionable information as a fact-based decision making tool for executives and their teams. This led to more effective Security Management at a lower overall cost and paved the way for more innovations in the Security Management arena.

Software helped to bridge the gap between the legacy of basic Security (standalone products and solutions designed to provide Security Effectiveness) -- and the delivery of more advanced (integrated) solutions that provided risk protection and even business value that transcended the scope of traditional Security. Software integration was a key enabler in gaining more quantifiable value and correspondingly, in more easily quantifying the associated ROSI in modern Security infrastructures.

In large corporations, the availability of more actionable information than ever before meant the ability to operate proactively versus constantly reacting to threats. Software-driven solutions delivered not only the means to collect information, but also equipped operators with the necessary facts for them to prevent events from happening in the first place. Software-driven solutions offered an alternative to traditional product-based systems – one that facilitated the sharing of data via a shared infrastructure.

Calculating ROSI

There was still a problem. Existing methods for calculating ROSI were complex and included a mind boggling array of mathematical formulas and statistical analyses. These calculations frequently relied upon “soft data” to derive hard numbers associated with ROI, making the challenge even more difficult.

The list of considerations and measurements suggested for these calculation methods was long:

- The Security professional could catalogue incidents resisted;
- He could note incidents survived;
- Equations could include assessments of best practices training costs and assigning monetary values to the time needed for implementing awareness efforts;
- Commitment costs could be calculated or the number of participants per day in Security workshops could be counted;
- A calculation might include enumerating disclosure efforts and the associated monetary sacrifice; assessing cleanup costs; cataloguing lost opportunities or even determining resistance to best practices.[1, 2, 4, 5]

Security professionals quickly realized that understanding these detailed methods and applying them to their respective businesses could take quite some time.

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.

A major car manufacturer couples optical turnstiles with access control devices at each vehicle assembly line to ensure that the appropriate headcount of qualified staff exists at the assembly line before production is started. This guarantees that the production line is staffed with the proper number of skilled workers, thus reducing the risk of costly mistakes and quality compromises that could otherwise occur.

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]

Security's holistic impact on a Buildings Strategy

When Security is one of many integrated management systems within a building or an enterprise-wide facility infrastructure, significant opportunities arise to drive energy savings. For instance, Security systems can deliver specific people-based occupancy information to a Building Management System, thus enabling that BMS to optimize its energy management routines. Based on business rules in the system, heating and cooling can automatically be shut off in an area of a building that is determined to be unoccupied. This delivers significant savings in both energy and hard costs. Security systems also can add predictive information about staff in a building and the areas to which individuals are assigned.

Another way in which Security technology can holistically impact overall building management is in the ability to provide headcount data for use in various business silos. Facility managers can use "time and date stamp data" captured from the credentials of the people admitted to a facility. This information may be applied to analysis and space utilization planning activities. They can also make use of that actionable information as they efficiently map space and lease property. This represents significant cost savings for the business.

On a daily basis, headcount data can also be applied to functions such as cafeteria management. Data from an access control system can be provided to food service staff at a certain time every morning to help streamline meal planning and production. Cafeteria staff can accurately gauge quantities, reduce waste and better control energy use and costs.

Internal forces such as specialization, mobility and globalization create opportunities for Security leaders to guarantee – and prove -- strong ROSI. Security as part of a broad holistic buildings strategy also provides the possibility of significant Return on Security Investment.

Convergence, the synergy between people, process and technology, also plays a significant role in deriving clear business value from the application of Integrated Security Management Solutions to real business challenges.

Convergence and the Security Lifecycle

In making Security an essential part of corporate DNA, executives must consider the synergy between people, process and technology. When all three work together in this intentionally designed symmetry known as Convergence, an organization can realize the highest possible performance improvements and reap significant benefits across many business operations.

Viewing the discipline of Security as a process-driven lifecycle highlights how this synergy from Convergence works as shown in Illustration 2.[14]

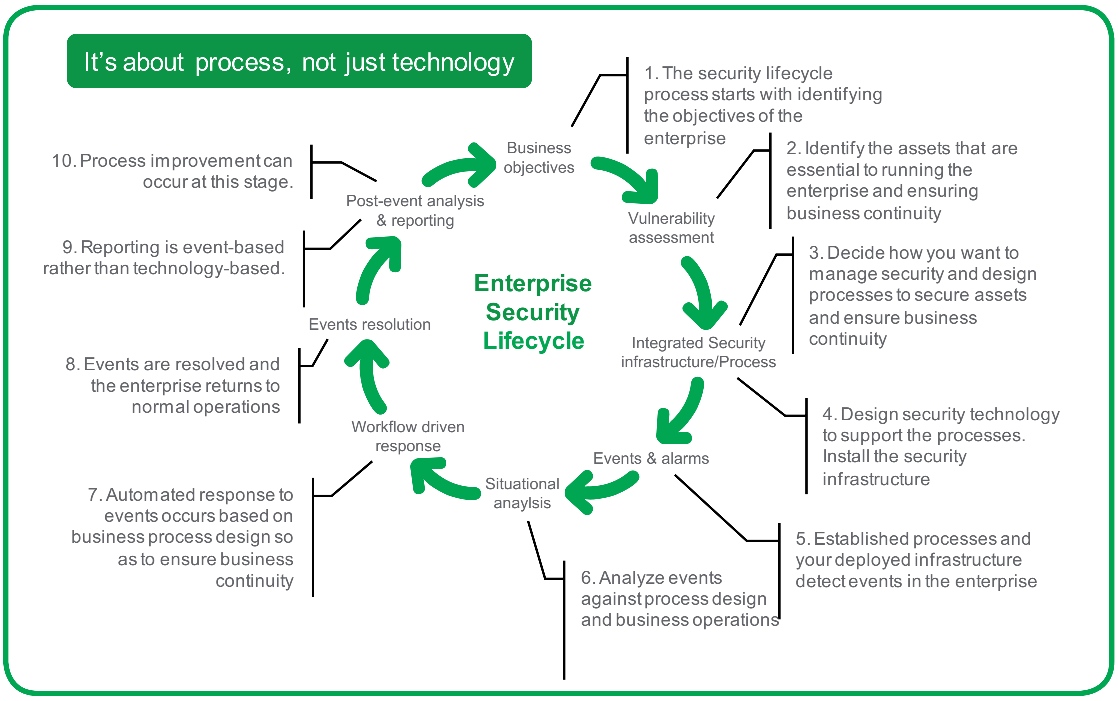
It's about process, not just technology
Enterprise Security Lifecycle
Business objectives
Vulnerability assessment
Integrated Security infrastructure/Process
Events & alarms
Situational anaylsis
Workflow driven response
Events resolution
Post-event analysis & reporting
1. The security lifecycle process starts with identifying the objectives of the enterprise
2. Identify the assets that are essential to running the enterprise and ensuring business continuity
3. Decide how you want to manage security and design processes to secure assets and ensure business continuity
4. Design security technology to support the processes. Install the security infrastructure
5. Established processes and your deployed infrastructure detect events in the enterprise
6. Analyze events against process design and business operations
7. Automated response to events occurs based on business process design so as to ensure business continuity
8. Events are resolved and the enterprise returns to normal operations
9. Reporting is event-based rather than technology-based.
10. Process improvement can occur at this stage.

Illustration 2 The Security Lifecycle: incorporating processes to ensure business continuity

The Lifecycle follows a progression chronologically through the eight stages that occur in most Security environments – from determining business objectives at the beginning -- to events resolution and post-event analysis and reporting at the end. Each of these stages provides a mechanism for continuous improvement on the part of the business's Security Management team. At various points along the stages in the Lifecycle, Security professionals can answer basic questions that are crucial to guaranteeing effective protection of the organization:

- What needs protecting: people, property or data?
- How are the people or assets potentially vulnerable?
- What forces are likely to attack the organization?
- How would such an attack be executed?
- How would such an attack be detected?
- How should our organization respond to an attack or disruption to business (e.g., in the case of natural disaster)?
- What reports are required to meet regulations or protect the organization from legal liability in the case of an adverse event?
- How should Security technology be deployed to support this?

Notice that the technology question is the last one. This a key point. The reason for this is that Security Effectiveness is as much about process as it is about technology. The investment in technology is made to support the processes that are established to govern how Security functions are carried out in the organization.

Now let's take a closer look at the Security Lifecycle and how its logic can be applied to the business of managing Security. The Lifecycle progression helps professionals in:

- identifying and articulating the objectives of the enterprise;
- identifying the assets that are essential to running the enterprise and ensuring Business Continuity;
- deciding how to manage Security and designing processes to secure assets and ensure Business Continuity;
- designing Security technology to support processes and installing the appropriate associated Security infrastructure;
- establishing processes and deploying infrastructure to detect events in the enterprise;
- analyzing events as compared to process design and business operations;
- reviewing automated responses that are based on the business processes design;
- resolving events and returning the enterprise to normal operations;
- reviewing event-based reports;
- implementing continuous improvements to processes.

In the Security Lifecycle, technology serves as a crucial enabling tool that can be designed in concert with the needs and goals of the organization. It provides situational awareness; automates processes; provides a platform for establishing rules that automatically analyze what is happening in the business; and flags anomalies as events. Technology helps Security teams respond in a planned and effective manner. Technology also enables reduced costs to be realized over the long-term. With the right technology, a Security team can increase the effectiveness and efficiency of Security and the quality of protection provided for the organization.

What’s next in Security

Security Directors and Facilities professionals will face even greater challenges in the years to come. As their roles change – and the Security Industry as a whole evolves, there are many factors that will be important to ensuring ROSI. In an asmag.com December 28, 2011 article, “Schneider Electric: 12 for 2012,” by Aaron Kuzmeskus, twelve key points for improving the bottom line are enumerated.[8] These considerations are paraphrased below.

Closing the ROI gap or monetizing Security

This entire paper has made the case for showing the high value Security brings to the business. With each respective level of Security (as described on pages 6-10) the monetary value placed on Security has the potential to incrementally increase. Over time, using Security as a business enabler will become more and more prevalent, especially in terms of applying Security technology to improve business processes in industry segments ranging from Manufacturing to Healthcare to Education. Security then transitions from being viewed as “a cost center” to being seen as a “profit center.”

Scalability

Security Management Solutions must be an essential part of adaptable, smart, comfortable, efficient and safe facilities. Integrated Security Management makes it possible to have a common control platform that enables operators to be more efficient and exceed today’s needs. It also provides the future-proof technology that allows businesses to change with what tomorrow brings.

Integration

Security command centers rely upon multiple applications to secure a facility. Each application — from access control and video surveillance to intrusion detection, voice intercom or biometric enrollment — typically has its own user interface, reporting process and audit trail. Systems that have “pre-integrated” management systems reduce equipment costs, energy usage and operator costs. They provide great benefits in terms of ease-of-use.

Interoperability

Security and Building Management software can automatically detect and communicate compatible devices at the IP level without the need for a communications gateway. By leveraging Security and Building Automation Systems, significant cost savings can be realized in terms of simplified a system architecture, less hardware, software configurations that require less programming and less complex systems operations and maintenance.

Simplicity

Flexible user interfaces with role-based menus are simple and intuitive, and relate well to typical, real-world Security situations. When combined with workflow management by job function, they reduce training time and help make operators more efficient and more productive. These user-friendly control platforms can also contribute to reducing employee turnover.

Green Security

Security Management and Building Automation should be integrated to improve energy efficiency and Security. The key is that those in the Security function not only know when someone is present, but also, they know the identity of that individual. If that information is applied to enable new energy routines in the building management software, incremental energy savings can be realized.

Reliability

Systems that feature distributed intelligence down to the local device level of every controller enable stand-alone control and offer the greatest degree of system reliability. Controllers that can run their own programs, logic, schedules, and trends as well as issue their own alarms and events maintain the needed level of operation — even when communication to the server is interrupted.

Information Technology

While once an optional part of the corporate infrastructure, IT-based systems now are essential to sharing information across a wide geography. They enable truly global operations. Many systems can function over a common IT infrastructure, removing the cost of separate system cabling.

Go wireless

Today's common advanced encryption and mesh network equipment can be deployed faster and more cost-efficiently than hard-wired installation, without impacting the Security or availability of the network.

Cloud

Everyone is talking about the cloud. What is it? Simply put, it is a shared service that can provide data storage or processing capability in a "virtual" environment. To subscribers, this means decreased capital expenditures, and in many cases better uptime reliability.

Analytics

Video analytics can also provide an effective way to maximize operational efficiency. Analytics can help identify video that should be monitored, based on activity, and analytics provide many powerful forensic tools as well.

Awareness

Physical Security Information Management (PSIM) is a powerful tool. By bringing many disparate sources of data into one set of actionable information, gains in efficiency and reliability can be realized — throughout the enterprise. This improves overall Security effectiveness.[8]

More to watch in the future

As we've seen before in the evolution of the Security Industry, the business model for the delivery of Security mirrors that of the service-based business model used in the IT Industry. As indicated by the technology shift from analog to IP, Security now operates as an IT business. The involvement of the Chief Information Officer (CIO) or the IT Director is common in the Security purchasing cycle. IT professionals bring business expectations from the IT world with them, including the requirement for competitive product pricing; the desire for a wide selection of technology choices; the need for a plethora of services such as routine software maintenance; and the desire for managed services. These expectations change the way Security Management Solutions are evaluated and purchased.

Managed services -- transferring the day-to-day responsibility for managing Security technology from organizations to outside service providers (other companies)[9] -- is becoming more widespread in the Security world. A good example of this concept is Software as a Service (SaaS) in which the software for managing video and access control is licensed to an organization, yet delivered over the Internet from remote locations. In this scenario, the initial cost is negligible. Over the long-term, the end user pays for only the Security services consumed.[3] Video as a Service (VaaS) is a similar trend.

As Managed Services become the norm, the value of this Security investment will be easier to quantify. Managed services will enable more (and better) Security technology to be affordable for more end users. These services will take the form of IT-based, network-friendly enterprise solutions that do not need to reside in an organization's own enterprise or on its own network. The services place a heavy burden on IT budgets.

Managed Services, or the "fee for performance model," works well in rapidly-growing multi-location large enterprise environments. In this scenario, an organization pays a single fee for the use of Security infrastructure over a long period of time -- typically three or five years. The Managed Service Provider (MSP) assumes total responsibility for the installation, maintenance, and performance of that infrastructure. The corporate end user can focus on the practice of Security (its core competence) rather than on the management of Security technology (not its core competence). In this arrangement, the end user and the service provider work together to strategically plan how Security technology should support business operations.

The Managed Services concept will open doors in terms of calculating ROSI. This business model returns working capital to a company's core business. In a Managed Services environment, Security hardware is leased, rather than purchased, as it typically is today. Service Level Agreements (SLAs) are implemented to ensure reliable operation of the Security infrastructure. This decreases the overall cost of Security for the end user. Thus, this strategy makes it straightforward to calculate ROSI.

Imagine an organization that maintains eighteen facilities in one city. Before deploying mobile and remote services, the company posted contract guards at each facility and relied upon guard teams to locally monitor alarms and video surveillance. Guards themselves decided which events required personal responses.

The guard staff was then replaced with a Managed Security services model that includes a central monitoring station that prioritizes calls and shares video data with vehicle-based responders. The responder team now is comprised of eleven individuals, a decrease in headcount by thirty one. On-site facilities in each building are no longer needed to house Security staff. In addition to the cost savings associated with the reduction in headcount, the business has reallocated previously required valuable floor space to meet other business needs.

Conclusion

The Security Industry has evolved considerably since 2009. Thanks to technology advances and thought leadership from Security visionaries, the discipline of Security Management now is solidly positioned as a business enabler. In its newly elevated role, it has become a critical element in holistic buildings strategies.

Those at the C-level who seek justification for Security Management purchases now can clearly see the inextricable tie to business enhancements, process and service improvements, energy savings, cost reductions, Business Continuity and sustainability. The technology and infrastructure that Security professionals so desperately need is supported by increasingly clearer use cases in all areas of the business.

Today, it is clear that Security positively impacts the bottom line. It is also easier than ever before to prove Return on Security Investment with tangible real life examples and hard numbers.

Appendix

1. Software Engineering Institute, *Calculating Security Return on Investment*, by Don O'Neill, (c) 2007 Carnegie Mellon University, https://buildSecurityin.us-cert.gov/bsi/articles/knowledge/business/677-BSI.html, accessed November 24, 2011.
2. CIO online, *Calculating Return on Security Investment*, by Scott Berinato, Feb 15, 2002, http://www.cio.com/article/30856/Calculating_Return_on_Security_Investment accessed November 24, 2011.
3. SearchCloudComputing, *Software as a Service*, no author noted, March 2006, http://searchcloudcomputing.techtarget.com/definition/Software-as-a-Service, accessed November 24, 2011.
4. CSO Online, *Calculated Risk: Return on Security Investment*, by Scott Berinato, December 9, 2002, http://www.csoonline.com/article/217727/calculated-risk-return-on-security-investment, accessed November 24, 2011.
5. *Return on Security Investment (ROSI)*: A Practical Quantitative Model, no date, http://www.infosecwriters.com/text_resources/pdf/ROSI-Practical_Model.pdf, accessed November 24, 2011.
6. *Finding the ROI in Security*, (presentation) delivered by Jim Sandelin at Expo Seguridad Mexico (ESM), by Jim Sandelin, Kevin McCaughey, Alex Mathieson, Aaron Kuzmeskus and Kathy Holoman, April 2011.
7. Today's Facility Manager, *Closing the ROI Gap in Security*, by Jim Sandelin, September 2011, http://www.todaysfacilitymanager.com/articles/services-and-maintenance-together-as-one.php accessed December 22, 2011.
8. asmag.com, *Schneider Electric: 12 for 12*, source: Schneider Electric, Aaron Kuzmeskus, December 28, 2011, http://www.asmag.com/showpost/12561.aspx, accessed January 3, 2012.
9. Wikipedia, *Managed services*, no author noted, December 15, 2011, http://en.wikipedia.org/wiki/Managed_services, accessed December 28, 2011.
10. SDM, *The Business Intelligence Value-Add*, by Heather Klotz-Young, October 12, 2011, http://www.sdmmag.com/articles/87013-the-business-intelligence-valueadd, accessed November 23, 2011.
11. asmag.com, *Efficiency Gains Achieved Through Integration*, source: Gary Tang, November 15, 2011, http://www.asmag.com/showpost/12388.aspx, accessed November 23, 2011.
12. asmag.com, *What's Next for the Industry? (Part I)*, source: Ling-Mei Wong, November 23, 2011, http://www.asmag.com/showpost/12428.aspx, accessed November 23, 2011.
13. asmag.com, *What's Next for the Industry? (Part II)*, source: Ling-Mei Wong, November 23, 2011, http://www.asmag.com/showpost/12429.aspx, accessed November 23, 2011.
14. Various Integrated Security Presentations, source: Kevin McCaughey, Schneider Electric, 2011.
15. *Security*, (Presentation), Schneider Electric Global Leadership Forum, source: Kevin McCaughey and Dave Berardi, Schneider Electric, January 2011.

This page intentionally left blank

This page intentionally left blank

This page intentionally left blank

Schneider Electric

One High Street,
North Andover, MA 01845 USA
Telephone: +1 978 975 9600
Fax: +1 978 975 9698
http://www.schneider-electric.com

♻ *This document has been*
printed on recycled paper