Integrated Security Solutions:

Securing our nation's critical infrastructure and key resources

More than any other type of enterprise, Critical Infrastructure and Key Resources (CI/KR) are vital to the security and economic prosperity of our nation.

Being entrusted with some of our country's most valuable resources and commodities is a serious undertaking. The potential implications of security breaches are immense and the resulting economic impact could last for decades.

The responsibility of Chief Security Officers and Security Executives at CI/KR enterprises is simply beyond the comprehension of the average security professional.

The nature of these operations – their size, complexity and nuances – is on a scale much different than the vast majority of businesses. It requires a different way of thinking, a more sophisticated security solution that will mitigate vulnerabilities and protect critical assets.

Integrated Security Solutions can have a transformative effect on the way you do business, allowing you to achieve real situational awareness, secure assets and add to core business – ultimately make your job easier.

There is a lot at stake. In order to fully appreciate the scope of the issue, it is important to examine all of the challenges involved. This white paper will identify those challenges and offer a comprehensive solution that you can use to make the right decisions for your enterprise.

Framing the issue

In the midst of the recent economic crisis, the phrase "too big to fail" was used to describe some of the investment industry giants the U.S. government chose to bail out. The same could be said of CI/KR. According to the Department of Homeland Security (DHS), these assets are so vital to the U.S. that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof.

(http://www.dhs.gov/files/programs/gc_1189168948944.shtm)

Take for example, the United States transportation system.

Counting airports, and the total kilometers of public-use paved roads, railways, waterways and pipelines, our nation's freight transportation network is the most extensive on the globe.

(http://www.bts.gov/publications/freight_transportation/html/table_03.html)

According to the U.S. Department of Transportation's Research and Innovative Technology Administration (RITA), transportation-related goods and services contributed $1.38 trillion to the $14.44 trillion U.S. Gross Domestic Product in 2008.

(http://www.bts.gov/publications/pocket_guide_to_transportation/2010/html/chapter_05.html)

White Paper

www.usa.siemens.com/iss

SIEMENS

System Mileage within the Unied States - 2008
(Statute miles)

Highway	4,042,778	Heavy rail	1,623
Class I Rail	94,082	Light rail	1,397
Amtrak	21,178	Navigable channels	25,320
Commuter rail	7,261	Oil pipeline	169,422
		Gas pipeline	1,530,012

Now consider the additional 19,930 airports, 3,000+ rail stations and 257 lock chambers across the country. Somewhere in the U.S., there are Security Executives responsible for safeguarding these operations.

(http://www.bts.gov/publications/national_transportation_statistics/#chapter_1)

Another example is civil aviation.

In 2007, U.S. airspace handled more than 767 million passengers, 836.3 billion revenue passenger miles (RPM) and 61.1 million aircraft operations. In the same year, foreign and domestic air carriers flying through U.S. airspace transported over 67 billion revenue ton miles (RTM) of freight, and U.S. carriers alone accounted for 39.7 billion RTM of freight and mail.

The FAA Forecast projects North American passenger volume and RPM to annually grow 2.2 percent and 3.1 percent, respectively, between 2009 and 2025.

Economic impact of commercial aviation on the U.S. economy

Economic Output	$1.225 trillion
Contribution to GDP	$731 billion
Share of GDP	5.2 percent
Job Impact	10.9 million

(Source: FAA Air Traffic Organization, *The Economic Impact of Civil Aviation on the U.S. Economy*, December 2009 ©1995-2010 Air Transport Association of America, Inc. All rights reserved.)

Nearly all shipments require the use of more than one mode of transportation to reach their final destinations. A shipment of imported goods arriving at a maritime port is transferred to rail or truck to continue its journey. Likewise, goods transported by rail will likely make part of their journey by truck.

The direct impact of these operations is considerable. Scheduled and non-scheduled transport would drop, resulting in declining sales. The replacement of parts and components would slow, and fewer operators and service providers would be needed, decreasing payroll across the board.

A significant security breach could cost millions over an extended period of time.

Now consider the indirect impact that the loss of an operation of this scale would have. The expenditures normally made by passengers and operators would dry up. The ripple effect of lost sales and salaries of many associated industries could be devastating to the local economy.

Market drivers

There are a number of issues that are creating added pressure and a sense of urgency among Security Executives.

ARRA funding

The American Recovery and Reinvestment Act of 2009 (ARRA Public Law 111-5) was designed to jumpstart the U.S. economy while addressing some long-neglected and challenging projects important to the nation. Funds received under this Act are subject to unprecedented levels of transparency, oversight and accountability. It is incumbent upon Security Executives to assess their current level of preparedness and determine if ARRA funding would be appropriate to their operation.

The DHS prioritized the ARRA projects that would infuse resources into local economies while meeting critical security needs.

The grant programs are divided into three categories to further strengthen the nation’s ability to protect critical infrastructure and transit facilities, and to assist fire departments. Together, the grants fund a range of preparedness activities centered on capital projects, operational packages, equipment acquisition, and new or upgraded fire stations.

Funding for the program has been allocated as follows:

ProgramFY 2009 ARRA	Funds Available
ARRA Transit Security Grant Program (TSGP)	$150,000,000
ARRA Port Security Grant Program (PSGP)	$150,000,000
ARRA Fire Station Construction Grants (SCG)	$210,000,000
TOTAL	$510,000,000

As long as funds are available, corporations will – and should – attempt to obtain them.

Disparate technology
Industry publications are rife with declarations of the need to upgrade technology to keep enterprises secure. While many would gladly purchase the latest and greatest innovation and all of the associated bells and whistles, very few have budgets that would allow for such an expenditure.

Truth be told: many pieces of analog equipment continue to perform adequately. However, there are a number of issues associated with the interoperability of analog, digital and IP technology.

- There remains a lack of communication between various pieces of equipment, particularly when those pieces are produced by competing manufacturers.
- The number of different data formats utilized in security remains sizeable – and grows with the development of new technology.
  - Video
  - Audio
  - Data
  - RF
  - Compressed
  - Uncompressed
  - MPEG
  - Composite
  - Component
  - Stereo
  - Mono
  - Digital
  - Analog
- Time is wasted and data is sometimes lost when it must be interpreted or retrieved manually, or moved from desktop to desktop. These system silos are inefficient and, as a result, overall situational awareness suffers.
- All of the requisite interfaces that must be purchased to achieve interoperability can increase the number of pieces of equipment in a system exponentially. Putting a system in place to address this issue, once-and-for-all, would be optimal.

How do security executives manage the quirks of each of these formats, and those created when trying to combine them, without compromising security? Should security executives go along with the break/fix mentality of the past or try a different approach?

Aging products and infrastructure
Just how old are the individual components in your security system? The cameras? The readers? The network? If your operation is like most, chances are, there are a few pieces that are past their prime.

There are no rules about the life expectancy of network equipment because it varies widely due to a number of factors. Network World determined that the average life expectancy of network-based, all-in-one security appliances is 3.5 years. Yet, in security, there is a generally accepted five- to 10-year life expectancy of a security system. There are also a number of upgrades, additions or repairs that can be expected. And when a change is made, is any consideration given to the impact that the change may have on other parts of the system?

http://www.networkworld.com/supp/2005/tips/112805-lifecycle-tips.html

Compliance
Whatever regulatory bodies you are governed by, each has a unique set of requirements and reporting procedures. All CI/KR enterprises must conduct business in cooperation with a number of regulatory bodies – federal, state and/or local. Security Executives must be conversant in numerous regulatory policies and up-to-date with the latest rulings in order to ensure compliance with each entity. Some of the most likely federal regulatory bodies include:

- Department of Homeland Security
- Transportation Security Administration
- U.S. Coast Guard
- Department of Transportation
- Federal Aviation Authority

Within each of those federal government entities there are myriad programs, acts and mandates, each with an additional set of criteria and reporting procedures. For example:

- Maritime Transportation Security Act
- CFATS
- Homeland Security Presidential Directives
- Transportation Worker Identification Card
- Certified Cargo Screening Program

Not only must you attain compliance, you must also prove it with supporting documentation. While reporting is a relatively benign activity, the threat of changes to regulations or reporting requirements is ever-present. It can be a mere annoyance, or a source for grave concern, depending on your operation.

The current economy
While the economy as a whole is recuperating slowly, it continues to wreak havoc on budgets.

For example, freight trains carried 20 percent less cargo last year than in 2008, according to a report by the Association of American Railroads, and the industry shed nearly 21,000 jobs. The 12-month period was the slowest since the association began keeping records in 1988. Less freight equals less revenue for everyone involved. (Freight trains carry 20% less cargo in 2009 than in the previous year, TRANSPORTATION, Jan. 14, 2010, By Ronald D. White.)

The current economic climate is also causing a rise in crime that Security Executives must anticipate.

In its 2009 Annual Cargo Theft Report, FreightWatch International announced that cargo theft industry-wide rose by 12 percent to an average of 72 cargo theft incidents per month, the most ever recorded. The chief executive officer of FreightWatch believes that a combination of factors, including the economy, has forced cargo theft gangs to become more aggressive and increase their active targeting of unprotected high-value loads.

(FreightWatch publishes 2009 Annual Cargo Theft Report By CCJ Staff Published January, 31 2010.)

Security Executives must have systems in place to prevent theft, as well as capture any relevant data that can be used to support the bottom line.

Current challenges

Protecting people, assets and infrastructure is exponentially more difficult in large-scale operations. The quantity of data generated, the number of staff involved, the amount of equipment required to secure operations can lead to information overload, actually making it more difficult to achieve real situational awareness.

In addition, there are a number of challenges that Security Executives must face:

Unfunded mandates

Unfunded federal mandates are not uncommon and many enterprises have devised ways to subsidize their implementation. For example, a review of the American Association of Port Authorities (December 16, 2008) Security Fees and Surcharges at U.S. Ports shows page after page of ports – from Baltimore to Corpus Christi to Portland – have assessed one or more fees to help recoup the costs associated with federal mandates.

Another unfunded mandate that must be met is the Transportation Worker Identification Credential (TWIC). TWIC was designed to provide a common identification credential for all personnel requiring unescorted access to secure areas of facilities and vessels regulated by the Maritime Transportation Security Act (and all mariners holding Coast Guard-issued credentials). After application and vetting, workers are issued a tamper-resistant Smart Card that contains his or her fingerprint and photograph, as well as a bar code and pin number to allow for a positive link between the card itself and the individual.

Originally, the Transportation Security Administration estimated 750,000 people would enroll in the program. According to the U.S. Department of Homeland Security, by mid-March 2010, more than 1.5 million workers have already been enrolled. Some companies are reimbursing the cost of TWIC to their employees.

One of the major problems with the implementation of the TWIC program is that not all required facilities have installed the proper scanners. The Coast Guard is expected to issue a mandate on card reader installation in the near future, making it a top priority on the lists of many Security Executives.*

Keeping up with unfunded mandates is challenging. Adding efficiencies and becoming proactive remains the goal.

Logistics

There are a number of factors that are simply part of the territory for Security Executives.

- Management and training of internal forces: police, first responders, technicians, program managers, etc., will remain a challenge.
- In a technologically dependent environment like security, aging infrastructure is a constant cause for concern.
- Security becomes increasingly complex based on the number of facilities and structures involved. Diverse facilities, those with multiple buildings and structures, perhaps spread over a wide region are inherently more vulnerable. Unless all subsystems are properly integrated, situational awareness suffers.

The ideal would be to find an enterprise-wide solution to unify and consolidate systems to help mitigate all of these factors.

Making the business case for security

Every company has competing priorities and traditionally it has been difficult to document how security can enhance business.

It is no longer sufficient to simply express needs, Security Executives must now create a solid business case for company stakeholders that justifies expenditures and proves ROI.

Many years after the introduction of the first pieces of computer-based security technology, the Security and IT departments continue to struggle with domain control. Any proposals must also assuage the concerns of the CIO and IT department.

When an incident occurs

Whether an intentional act of terrorism, or simply a turned-around tourist, any incident that occurs can cause a serious disruption to operations, and the cost can be enormous. The time lost and the associated costs then become a security issue.

Consider the consequences of an airport terminal evacuation. A professor of finance at the University of Denver's Daniels College of Business estimates the average cost of shutting down an airport for a day to be in the six figures.

(http://www.dailyfinance.com/story/when-the-cost-of-flying-safely-keeps-rising-who-pays/19433821/)

According to one aviation consultant, a two-hour shutdown of a major terminal at an airport like Chicago's O'Hare can cost an airline up to $15 million. Once an incident occurs, a cascade of expenses begins. Refunding tickets and transferring passengers to other carriers takes time and may require ticket agents to work overtime. Flight delays and diversions can cause planes to burn more fuel and increase costs for maintenance, cabin cleaning and catering.

(http://www.usatoday.com/travel/news/2005-05-10-evacuations-usat_x.htm)

If a non-threatening incident can run into the millions, what would be the cost of a catastrophic failure?

The numbers and circumstances may differ, but the same grave concern holds true for all CI/KR operations,

Missing opportunities

Security Executives continue to be frustrated by an inability to seize missed opportunities:

- Key breaches are occurring.
- Property loss/damage occurs to vehicles, equipment, piers, gates, docks and buildings, but security departments are often unable to assign liability without tangible proof.
- The resulting loss of use (vehicles, equipment, etc.) and business interruption causes further complications.
- Revenues such as docking and anchorage fees, ramp parking fees and tariffs are missed which could be used to support the business case for security.
- Missing other important data for use in supply ordering, production performance, designing best practices, employee attendance, etc.

Even the Maritime Administration Port Risk Management and Insurance Guidebook recognizes the missed opportunities:

Development of a Port Security Plan

"All too often ports address current problems, failing to identify future threats, resulting in reduced efficiency, increased cost, and most probably providing a solution that does not interface with the previous plan."

The solution: Integrated Security Solutions

Integrated Security Solutions is more than the mere installation of devices. It is a comprehensive plan for enterprise security. It is the strategic consolidation and integration of subsystems into a situational management plan; the ability to centralize access control, intrusion detection, command and control, PSIM and video analytics and stratify all of the data generated – to maximize your operational efficiencies. Turn information overload into action. It is security enabled flexibility.

Benefits

Perhaps the most important benefit of Integrated Security Solutions is the ability to put a framework around all of your operation's security issues. For the first time, Security Executives can be certain that all of their concerns, goals and business processes have been carefully considered and translated into actionable items.

Other major benefits include:

Cost savings
- Avoid costly shut-downs
- Reduce insurance rates with enhanced security coverage

Revenue generation
- Gain all revenues rightfully due
- Document accidents
- Assess related fines or assign liability to recoup losses

Improved responses
- Speed response times
- Increase apprehension rates
- Dispatch assets to prevent security breaches vs. reacting after the fact
- Limit false alarms

Operational efficiencies
- Achieve real situational awareness
- Deploy assets where most needed
- Track assets without escort – appropriate resources
- Document all breaches and evaluate response
- Redistribute manpower to critical areas, other tasks
- Gain a higher level of professionalism overall and become more attractive to your customers

Appropriate data usage
- Filter data for analysis
- Share information between business units
- Share critical information with external partners

Integrator requirements

The scope of CI/KR integration is beyond the ability of most vendors. These projects simply don't fit into normal market channels and a single branch can't deliver on these large-scale projects. There are too many nuances and compliance issues involved to risk partnering with the wrong integrator.

It is critical that you select an integrator with the following skill set:

Vertical market expertise
- Experience in your specific market
- Operational knowledge of mission critical environments
- Thorough understanding of regulatory requirements

Skilled, experienced workforce
- Minimum 10 years experience in the security industry
- Relevant industry certifications

Dedicated integration team
- Staffed with integrators vs. installers
- Experience with intelligent, multi-layered solutions

Consultative approach
- True partner vs. selling the latest gadget
- Learns your risk profile
- Understands your business

Sufficient operational resources
- Substantial size and assets
- Can deliver on economies of scale
- Global expertise

Process driven
- Offers business efficiencies
- Provides compliant solutions

Research & Development
- Investment in R&D demonstrates foresight into future needs
- Manufacturer/integrator is preferable

Product portfolio
- Sells solutions vs. products
- Offers best-in-class product portfolio from top manufacturers
- Provides custom software development
- Uses open-ended architecture

Outstanding customer support
- Superior service
- Sufficient service/maintenance staff
- Central monitoring option available

How it works

In order to demonstrate the effectiveness of implementing Integrated Security Solutions, consider these example scenarios:

Scenario 1

A security office monitoring RADAR at a major U.S. seaport detects a small water craft approaching at a high rate of speed. Applying intelligent video and analytics, he is able to determine that it is not a part of the port's own security force, nor any scheduled vessel. The craft does not respond to repeated attempts at communication. The Coast Guard is automatically alerted and deploys a scib (floating barrier) to prevent the craft from entering the port.

What if the craft had been loaded with explosives? How many lives could have been lost? What damage could have been done to the port's infrastructure? The environment?

With a carefully developed Integrated Security Solution, the port was prepared to prevent such a disaster and avoided any subsequent loss of productivity.

Scenario 2

The underground perimeter fiber at a global food manufacturer alerts security to an anomaly. Moments later, motion detectors indicate the fence line has been breached. Simultaneously, a camera is moved to the area to discover what has violated the perimeter. Appropriate resources are dispatched to apprehend the intruder.

Exactly where did the intruder go? Did he tamper with any of the company's product or ingredients?

In other circumstances, the company would have to destroy any products or supplies that were accessible to the intruder. With an Integrated Security Solution, the intruder's movements can be retraced to prove or disprove tampering.

Scenario 3

In the middle of the night a tank ruptures at a chemical treatment plant. Since the plant tied their environmental sensors to their security system, and outsourced their monitoring function, the Central Monitoring Station immediately notifies the customer of the rupture. Pre-programmed rules and links to building automation turn on the exhaust system.

What if the customer had not received immediate notice of the failure? What if the exhaust system had not been activated?

A value-added benefit of a comprehensive security plan helped mitigate losses and put disaster recovery efforts immediately into motion.

In security, success is often measured by what doesn't happen. With Integrated Security Solutions, every component of a security plan is fulfilled:

- Multiple sub-systems are integrated into a single GUI.
- The system responds instantaneously to any trigger.
- Computer-aided dispatch deploys the appropriate resources immediately.
- The system is resilient and provides seamless redundancy in the event of a breach.
- CCTV, access control, perimeter protection and other systems are no longer trapped in silos, but are brought together and put into context. This new intelligence is used to improve business productivity.
- Security becomes proactive.

The Siemens solution

In the crowded market of security, Siemens is the only integrator to make a significant investment in Integrated Security Solutions.

Our dedicated team is comprised of industry veterans from critical infrastructure with an average of 27 years experience in security. Each member has undergone additional Siemens-specific security training and has all relevant industry certifications, including Project Management.

We use a consultative approach and develop systems that fit your business and risk profile, planning for current needs and beyond so today's investment remains relevant tomorrow. We offer the vast resources of our entire operation through a single point of contact to develop compliant, scalable, customizable security solutions that help improve efficiencies and save money.

Siemens does not sell out-of-the-box products. We sell solutions – products and services bundled in a way that's unique to you. As the largest security systems integrator in North America, we have a powerful portfolio using best-in-class products from top manufacturers in the industry. Our portfolio also includes Siveillance™, our intelligent video, and command and control family of products that are customizable and can be integrated to create complete situational awareness.

To learn more about Siemens Integrated Security Solutions offerings and how they meet the most complex security demands, schedule a meeting with one of our security professionals today.

Go to: ~~*http://www.buildingtechnologies.siemens.com/bt/us/Services__and__Solutions/electronic_security/security_specialists/Pages/IntegratedSecuritySolutions.aspx*~~

Siemens Industry, Inc.
Building Technologies
1000 Deerfield Parkway
Buffalo Grove, IL 60089
847-215-1000

Siemens Canada Limited
Building Technologies, Security Solutions
2 Kenview Boulevard
Brampton, ON L6T 5E4
Canada
905-799-5990

Printed in USA

www.usa.siemens.com/security
www.siemens.ca/buildingtechnologies