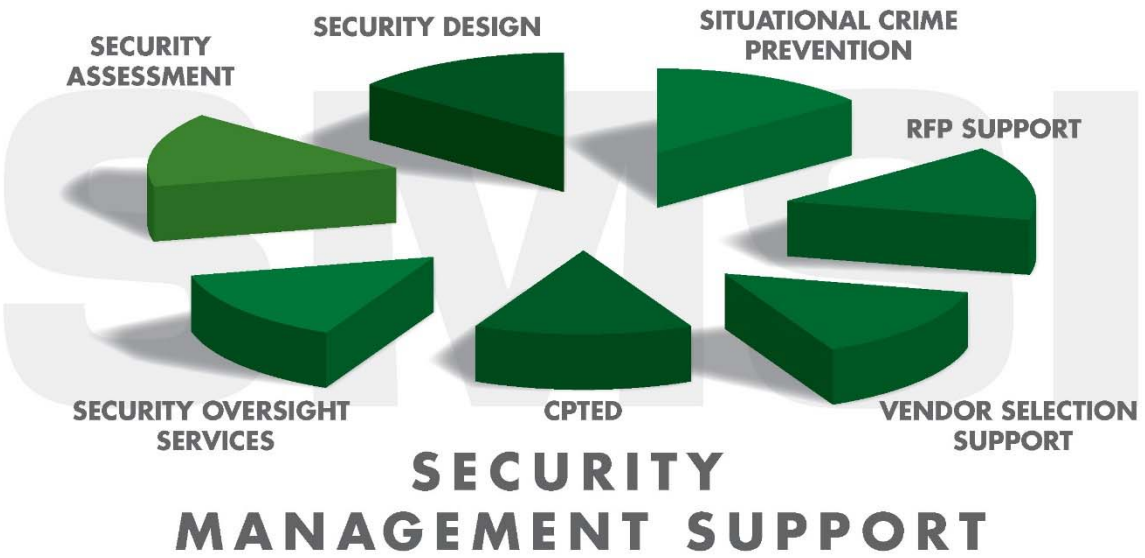
SMSI, Inc. • 1168 Pan Court • Newbury Park, CA 91320 P 805.499.3800 E bill@smsiinc.com

Security Management Support Program for Healthcare Facilities



SMSI Inc. (Security Management Services International, Inc.) has been serving the Healthcare industry for over 30 years. These services have primarily been comprised of the provision of comprehensive security assessments, and to a lesser degree, our retention as court-certified forensic security experts. Our caseloads have included homicides (patient & staff), infant abductions, active shooter events and sexual assaults. Each of these cases continues to inform us that hospital security programs must substantive, with measurable results, to be effective.

The purpose for drawing attention to our litigation experience is convey the notion the that all hospitals hospital security programs have potential of legal consequence in the wake of failure. More importantly, the demonstrable benefits of effective security programs are always cost justified when litigation is avoided. Our considerable litigation experience has also made us keenly aware of the elements of potential causation.

From a clinical perspective, hospitals generally operate under the rubric of *universal precautions*. Universal Precautions are clearly an effective criterion for a wide range of clinical procedures. However, to apply this value system to security policies and methodologies is generally inappropriate. **Security is, and must continue to be, a situational discipline**.

The efficacy and design of security programs is determined by the understanding of the realities of the ambient threat environment. The threat environment for hospitals is

determined by a wide range of sociological and cultural factors. To mitgate security vulnerabilities, the threat environment must be continually monitored, followed by appropriate corrective adjustments. For these reasons, and others, security is, and always will be a **situational discipline**. Security programs must be dynamic and flexible to quickly adjust to fluctuations in the threat environment. Additionally, as security technology and methodologies evolve and improve, adjustments must be made. In other words, the reasonable standard of care doctrine is a dynamic discipline. The advancement of security technology has had a dramatic, positive impact on most hospital security programs, and that evolution continues. Technology continues, and at the same time, improve. For example, consider the positive impact that infant security systems have on the reduction of threat of infant abductions. Compare the current hospital statistics for infant abductions provided by the **National Center for Missing and Exploited Children** today, as compared to 15 years ago.

A vulnerability often overlooked by many hospitals is the adequate protection of consumable and fixed assets, as well as information (HIPAA). When this oversight occurs, cost saving opportunities are missed.

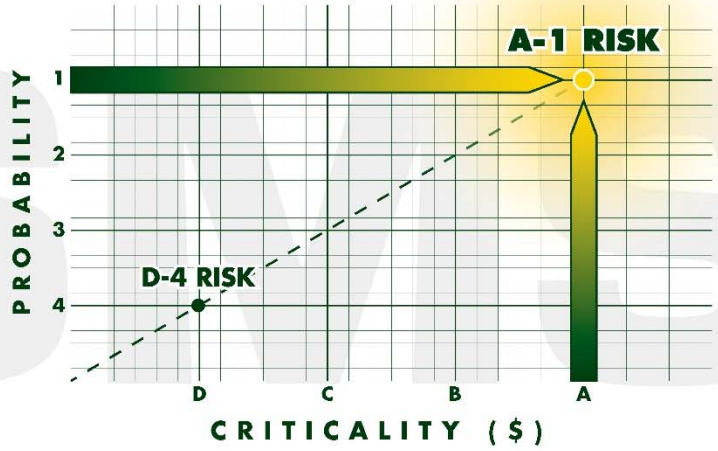
Finally, in the past few years we are seeing a flurry of attention being given, by numerous state and federal regulatory agencies, to the broad subject of **Workplace Violence (WPV)** mitigation. The accumulative effect of these actions has more clearly modified the expectation of a reasonable standard of care.
The well qualified **Security Management Support (SMS).** team is prepared to offer a wide range of security related services and expertise that are intended to identify and quantify the risk-mosaic at your hospital on number of different levels. Security is, and must, be site specific.

Once the initial security assessment has been completed, the **SMS Team** will put forth a strategic blueprint aimed at the mitigation of risks. The **SMS Team** will continue by helping to implement an agreed upon plan. Additional, this group (SMS) will support the creation of RFPs, the bidding process and the vendor selection process. Further, we will ensure that permanent onsite security personnel are sufficient trained and equipped predication on identified needs. This support is applicable to contract or proprietary security officers.

Security Needs Assessment

Because security is a situational discipline, every security program is distinctive and unique, predicated on needs analysis. This uniqueness is driven by cultural diversity, sociological diversity and a unique crime pattern diversity. In other words, the threat matrix for every hospital is unique. These preconditions, and many more, must be reflected within the design of each security strategy.

The first step of the **Security Management Support** process is to determine the security history of the hospital. This entails gaining an understanding as where the security program has been, where it is now, and where it needs to go moving forward.



VULNERABILITY ASSESSMENT MATRIX

This process requires an evaluation of the risk environment. As depicted above, the **Vulnerability Matrix** is unique for each hospital. All identified risk factors must be quantified as two dimensional: **criticality** and **probability**. **Criticality** is defined by the financial impact, should the identified risk comes to fruition. **Probability** is quantified by the statistical data that defines likelihood that an identified risk will come to fruition.

It is important to remember that Security is an anticipatory/mitigating discipline. Given the ambient threat environment, security programs should be designed for reasonable prevention. In support of the notion of quantification, this phase will also include the usage of a **CAP Index Crimecast Report.**

It is astounding how often security programs are put in place without an objective, quantifiable/comprehensive risk assessment. **Effective security programs must not be built on speculation and assumptions.** They should be the product of real data. Data should also be the backbone of the security program going forward. Remember. when it comes to security programs, the reasonable standard of care for hospitals is higher than almost any other industry that serves the public. When patients are victimized by crime: comparative negligence can rarely be applied to patients.

The SMSI Likert Style Questionnaire

The **SMSI Team** has created a unique assessment tool, the security questionnaire. Before and during the assessment process, access to this questionnaire is posted on the hospital's intranet-website. The employees of each hospital are asked to anonymously respond to this Questionnaire.

The **Likert Questionnaire** asks the respondent to reply to a number of statements by choosing on a scale of 1 to 5, Strongly Agree to Strongly Disagree. The questionnaire also invites comments (many of which are very revealing). The questionnaire implicitly sends the message to all employees: Your opinions are important to the process.

This Likert style Questionnaire, designed by the SMSI Team with need-driven modifications over the years, is an exclusive methodology. To the best of our knowledge, no other firm takes this approach. We have been using the Questionnaire for about seven years, and it has been well received and greatly appreciated.

A few years ago, a client in Georgia was not only pleased with our use of this instrument, but he has a basis of comparison. This CEO told us that he had recently commissioned a similar survey, using a vendor that specialized in these services. The client informed us that he paid over $12,000 for a similar survey, and our instrument was better and more informative, and it was included within our assessment process.

This Questionnaire has had many indirect benefits: **First**: we have found that when employees are invited to participate in the assessment process, they are appreciative that their voices are being heard and considered. When employees are invited to participate in the assessment process, we have found that these same employees are much more likely to buy into the subsequently recommended solutions. **Second**, because the Questionnaire

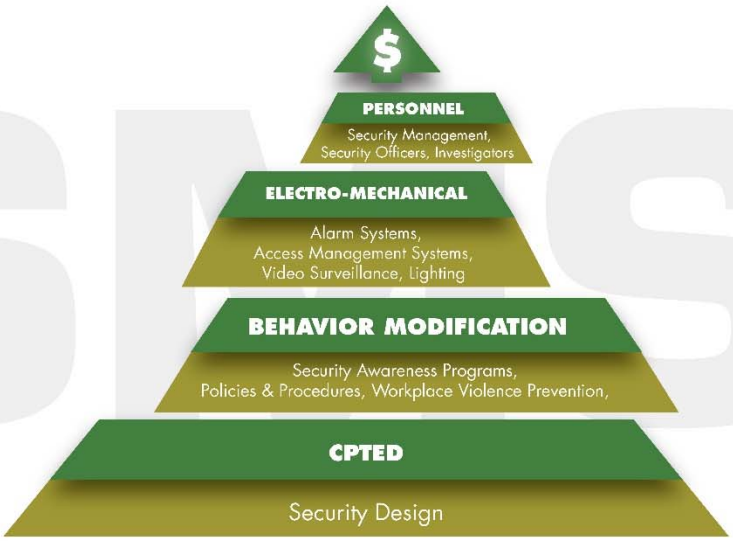
is always posted prior to our arrival, we can hit the ground running. **Third**, when we find a disparity between employee comments and reality on the ground, that information is still very enlightening, as to what is motivating responses the seem to fly in the face of reality. When perception does not line up with reality, the question becomes what is required to change the perception?

-This **Questionnaire** will provide **SMS Team** with a random sample of employee attitudes and perceptions at all facilities (applicable to multi-hospital organizations). *Typically, the questionnaire is posted in advance of our first onsite visit, on hospital's Intranet Site, and remains posted through the assessment process*. At the end of the process, the team will roll up our findings and provide a sample of relevant comments made by the participants. These comments will be presented in a manner to protect the respondent's anonymity. Once the Questionnaire is posted, we will immediately begin receiving emails every time a questionnaire is completed. These early responses often provide with a running sense of what areas require special probing.

We found that the questionnaire has become such a valuable tool,- in part, is because the respondent is allowed anonymity. This methodology is unique because it helps to measure both the reality of the security program, as well as the perception of the security program. As previously stated, the employee's participation guarantees their anonymity. In a recent assessment, we received more than 1,900 responses from a single hospital.

Again, this questionnaire allows the **SMS Team** to hit the ground running when they arrive on your campus, because it is posted prior to our arrival on scene. It provides clues and insights that we may have otherwise missed. It also provides us with areas of inquiry. We understand there will be some hyperbole and exaggeration. Even that information is helpful, because the question arises: "Why did they feel the need to say that?" The **SMSI Questionnaire** is probably one of the single best methodologies we have ever designed. We never give up thinking outside the box.

The Application of Security Solutions & Design



SECURITY SOLUTION HIERARCHY

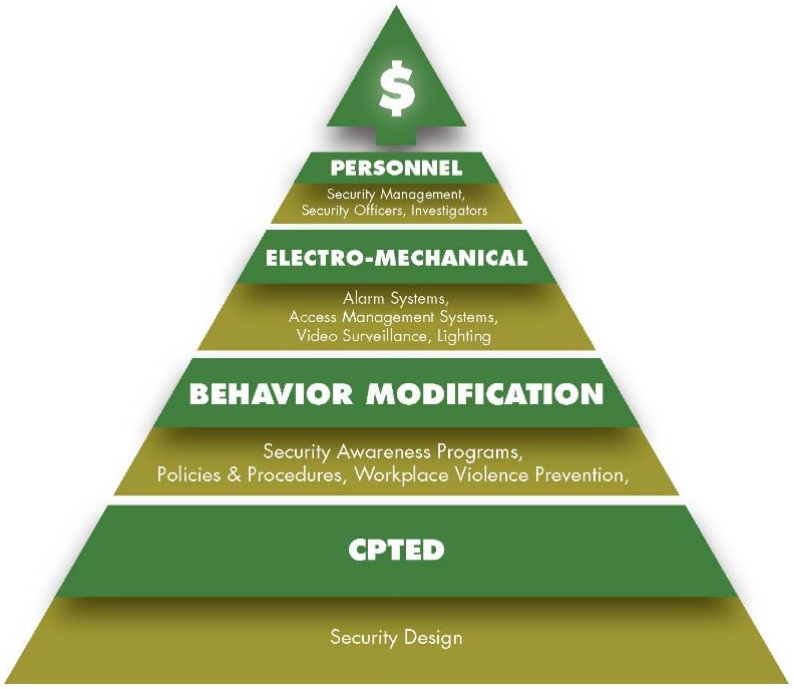
Once **SMSI Inc**. has defined the ambient threat environment, the next step requires the application of site-specific, reasonable remedies. The **Security Solution Hierarchy** defines and prioritizes four classes of mitigation. This hierarchy is patterned after Maslow's Hierarchy of Needs model.

The use of the **Security Solution Hierarchy** provides a theoretical roadmap fr the application of appropriate security remedies. This model provides a logical sequence for the application of security solutions predicated on identified needs**.**
Analogous to the original version of Maslow's Hierarchy of Needs the hierarchy provides the progression ending in self-actualization. If a person is lacking the basic needs for survival, self-actualization is a distant goal.

The Security Solution Hierarchy is a cost/benefit Hierarchy. This means that less cost remedies must be applied first, until optimal and cost-efficient security is attained.

The first level of Security Solution Hierarchy is **CPTED** (Crime Prevention Through Environmental Design) because it is the most cost-efficient remedy, and if properly applied, has the potential to reduce, or minimize the security budget overhead. CPTED illustrates the important role that perception plays in any effective security program

The second level, **Behavior Modification**, acknowledges the participation of employees as part of the solution, and the need for staff training.
We frequently ask employees they were asked to be aware of suspicious behavior during new employee orientation. When they respond in the affirmative; we ask them to define suspicious behavior, and often, they are unable to do so. We have found the less that one hour of training will fill a large void. Every employee should be encouraged to be part of the solution. Proactive employee involvement may have a significant impact on the reduction of security budgets.



The third level encompasses **Electro -Mechanical Solutions** such as fencing, gates, locking systems, access control systems, lock and key systems and video surveillance systems
The fourth level is associated with the use of **security personnel, including support functions such as: Security Officers, Security Department Supervisors and Managers, including patrol taxes and benefits.** This level has the greatest potential to invite security litigation. This model also supports the notion of cost effectiveness and efficiency. When the needs analysis is complete, this model will become whole in a manner that will assure that the **whole is greater than the sum of its parts**.

It should also be noted that there is a level of interdependency for each layer of the hierarchy. Additionally, as one moves up the hierarchy, each layer is reinforced by the subsequent layer.

In the real world, it is not infrequent that levels depicted here are turned upside down. In those cases, the first option is often the hiring of security officers.

The Application of CPTED Principals

Because **CPTED** is not widely understood, it will be briefly addressed here. Each pentagon depicted here, represent a component of **CPTED** design for hospitals. **CPTED** is applicable to the architectural design of hospitals, as well as landscape architectural design.

The application of **CPTED** principals is the first option on the **Security Solution Hierarchy**, yet often the least used. **Access Control** (**wayfinding** in **CPTED** language), should be a critical component of any hospital security program. Real and perceptual clues should guide invitees to common areas of ingress and egress, while discouraging pedestrian traffic from clinical areas.

Properly applied, **CPTED** is a cost-effective force and system multiplier, applicable to any security program. Security programs lacking **CPTED** consideration are less than optimal. Most **CPTED** design principals are very cost efficient and will improve almost any security program. In some areas of the country, the application of **CPTED** principals are required by code. **CPTED** can become the glue that holds security programs together.

For more information on CPTED, see Wikipedia. Wikipedia does a good job describing the history and application of CPTED principles.

Security Management Support

The Underlying Assumptions of Security Management Support (SMS)

Every hospital needs and deserves well qualified and experienced security management expertise. However, this expertise, and the associated payroll burden may not be required on a fulltime basis.

Because security is a situational discipline, the security and loss prevention program of every hospital should be unique as determined by specific needs. Additionally, hospital security programs must also be responsive to subtle changes in the ambient threat environment. Hospital security is a dynamic discipline. Cost efficiency, as determined by the **Security Solution Hierarchy**, is a must, especially for an already squeezed healthcare industry. The payroll burden for a well-qualified security team can be significant and reoccurring.

When it comes to security design for surveillance systems, access management and protection of sensitive and high value areas, expertise is required. Security expertise is a must for effective security design, as well as for vendor selection and oversight. Consider this: *If security vendors know more about what they are selling, than the customers know about what he/she is purchasing, where does the advantage lie?*

Management of Aggressive Behavior

The most effective security programs train all employees, at some level, in effective engagement and crime prevention behaviors, including the mitigation of aggressive behavior.

Security programs that are heavily dependent on uniformed security officers may be over spending with diminished return on investment. The partial answer to onerous payroll burden may lay with the use of technology, as well as the increased involvement of rank and file employees (internal crime prevention programs).

Over the past 20 years, security technology has vastly improved, and it has become very cost efficient. Services such as virtual patrols and virtual employee and visitor escorts represent just a few of the cost-effective options now available. There is real potential to improve your security program, while reducing payroll burden and while improving your security operation.

Finally, the Healthcare Security Management team will ensure that appropriate and qualified security officers are providing adequate return on investment, and that they are cost efficiently well integrated into a holistic security strategy.
The level of need for **SMS** will vary from one hospital to another. This variance will be determined by the level of threat and the level of need required for the reasonable mitigation of security risk.

SMS Deliverables

It is not the intention of Security Management Support Program to micro-manage the hospital's security program, but rather to support the mission of the Security Operation with our experience and expertise. Our mission is to cost effectively improve your existing security program, while at the same time ensuring that the program remains relevant and proactive to an ever-changing threat environment. Security programs are always in a constant state of flux. The two major factors are new and emerging threats, and the advancement of security methodologies, including evolving security technology. This service is intended to provide security management support while controlling costs and ensuring that security vendors are providing relevant and cost effective remedies.

Special Security Services

These services may include, but are not limited to:

- Set up of **EXEC Report** Daily Activity Logs and Incident Tracking System
- Security system design, RFP development &vendor selection support.
    - Access management systems
    - Perimeter security systems

- Visitor control
- Video surveillance system
- Proprietary and/or Contract Guard Services
- Special security systems
    - Infant security systems
    - Behavioral Health
    - Pharmacy security
    - ER security protocols
    - Business Office security system
    - Central supply
    - Tank farm
    - Loading docks
    - Parking facilities

The extent of the **Security Management Support Offering** will be predicated based on mutually determined needs, including emerging needs determined with the passage of time. Such needs may include:

- The implementation of employee Security Awareness Programs
    - Crime prevention
- The ability to prevent and mitigate aggressive behavior
- The development of strategies to better protect property
- The Development of Active Shooter protocols
- Sexual assault mitigation strategies
- Response to emerging trends identified by REPORT EXEC

<u>Potential Benefits Derived from Security Management Support</u>

- **Cost efficient security system design**
- **A need driven security program**
    - **Security officers**
    - **Electronic security systems**
    - **Video surveillance systems**
- **Enhanced employee participation**
- **Cost effective security budgeting**
- **Liability minimalization**
- **A safer campus**
- **Reduced management overhead**
- **The advantages derived from CPTED Design**

- **Ongoing threat assessment analytics**
- **Security vendor selection oversight**
- **A welcoming campus**

Report Exec as an Effective Security Management Tool

Security decisions must be data driven. *Without relevant and effective data, the means to quantify ROI is missed in favor of unverified hunches and speculation.* The tools required to accomplish these objectives will be applied because of our strategic partnering with **Report Exec.** The **SMSI** team has witnessed, over the past 25 years, the benefits derived from Report Exec. No longer are security program decisions clouded by speculation and built on bias and favoritism.

The **SMSP** team will be able to monitor the patrol and incident data as it is accumulated within the **Report Exec System**. We will have the ability to monitor time, place, situational factors and the people involved to recommend cost-efficient remedies, whether training, situational awareness, and/or needed behavioral adjustments.

Report Exec takes the guess work out of trend analysis. This program will also provide direct feedback regarding the efficacy of remedial actions in the face of new and/or emerging threats. Emerging information will also be available the monitors and the **SMS Team**. Corrective actions, taken in timely fashion, will negate the establishment of negative trends.

In the following section, **Report Exec** capabilities will be provided. The **SMS** team will work with **Report Exec** data to ensure that this security management tool is configured to meet the dynamic set of situational needs of every client. The use of a home-grown system compared to using **Report Exec** designed to meet your specific needs, is the difference between hunting with a rifle as compared to a shotgun.
The next section will address the parameters of the **Report EXEC** component of this service package.

REPORT EXEC

KEEPING HEALTHCARE FACILITIES SAFE

When stakes are high, people can be unpredictable. With violence in hospitals on the rise in recent years, your security team must be more prepared, organized, and alert than ever. With Report Exec, you can be.

Report Exec is a comprehensive incident management software suite for healthcare facilities. When incidents occur—any type of incident—Report Exec tracks all the details quickly through an easy-to-use reporting interface. The reports not only ensure that detailed records of incidents exist, they're also organized in a searchable database. Built-in analysis features make it easy to analyze the data collected in reports to identify patterns and trends, helping you work smarter to actually prevent incidents rather than just respond to them.

STATISTICS

Report Exec organizes data from your healthcare facility in an easy-to-search database. Pre-formulated statistical reports, customizable reports, and a live data dashboard provide all the statistical analyses you need to make more informed decisions.

COMMUNICATION

Built-in communication features help keep everyone on the same page and streamline operations. Customizable user roles and permissions ensure that everyone can access exactly what they need to effectively perform their duties, and nothing they don't.

EFFICIENCY

Report Exec eliminates time spent re-entering information by automatically populating known information. Quick-key codes and drop down menus reduce the possibility for human error while speeding up data entry and ensuring consistent reporting.

ACCOUNTABILITY

Securing your operating budget often depends on demonstrating the impact of your department, and the responsible allocation of resources. Report Exec records and organizes this information to justify budget requests and maintain transparency and accountability.

AUTOMATION

Save statistical reporting filters and set your ideal delivery schedule, and your reports automatically show up in your inbox. Automatic notifications for certain types of incidents or locations ensure that the right people are always kept in the loop.

25 MODULES

The comprehensive software suite includes everything a hospital security department needs to ensure a safe facility, and more. 25 modules to handle everything from visitor tracking to parking permits and dispatch makes Report Exec a game changer for hospital safety.

"The system is very easy to use even for those who do not have the sharpest computer skills. Creating incident reports is a breeze and running reports on the historical data is extremely easy as well."

-Barney McGrane
Northwestern Memorial Hospital

COMPETITIVE EDGE SOFTWARE, INC. | REPORTEXEC.COM | 866.421.2374
SALES@REPORTEXEC.COM | @REPORTEXEC

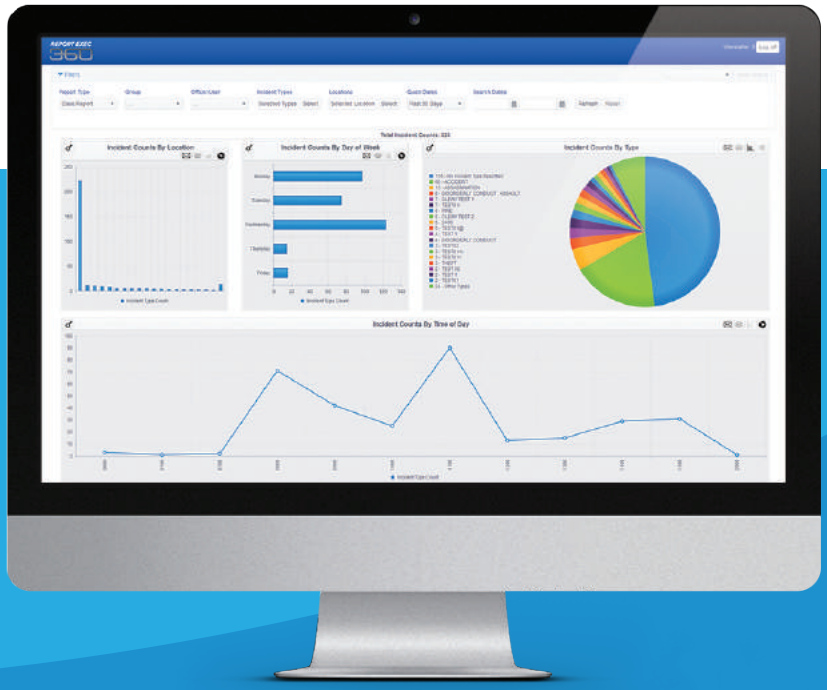
REPORT EXEC

SEE A BIGGER PICTURE OF SECURITY

Report Exec is a cloud-based public safety and security management platform

2017 Product Overview

If you can measure it, you can improve it.



With Report Exec 360, organizations can work smarter and be more proactive.

Report Exec's Data Analytics dashboard offers up-to-the-second security data analytics to measure the statistics that matter to you, and provide a high-level snapshot of your security landscape.

Get specific with your statistics using interactive visual data. Filter by incident types, locations, date ranges, users and more. With a single click, you can add or exclude data points and define the data sets that matter most. The simple drag and drop interface makes it easy to build reports and save them to your dashboard to monitor changes.

Monitor Trends

Identify Hotspots of Activity

Discover Patterns

Make Better Decisions—Faster.

How do you know if your security strategy is working?

With the 360 dashboard, you can set goals, track your team's progress using benchmark analysis, and monitor incident rates to measure the success of your initiatives.

Who else uses Data Analytics to monitor resources and results?

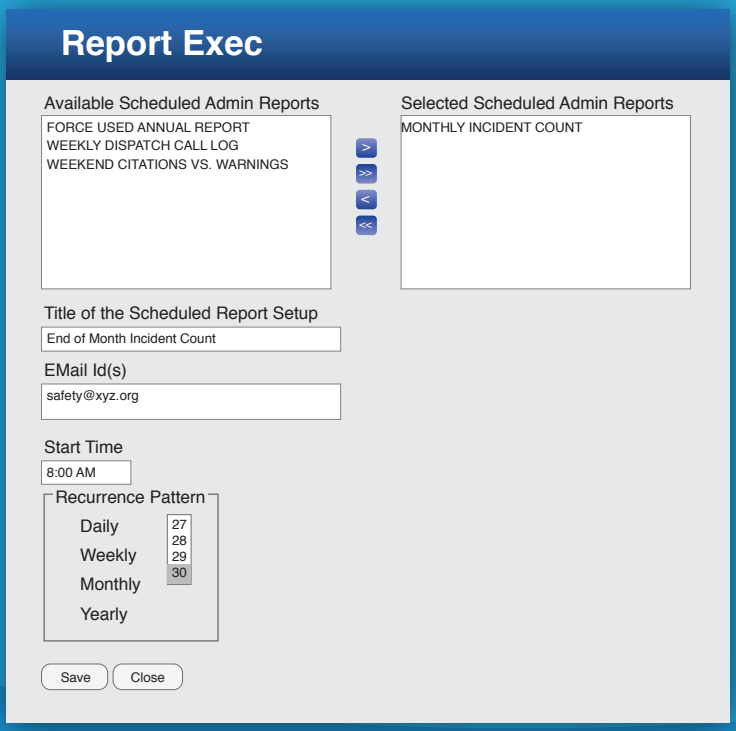
Today's world runs on data—hunches are no longer enough to justify action. Leaders in industries ranging from pharmaceuticals to government to retail are turning to business intelligence and data analysis to help them make better decisions faster.

REPORT EXEC www.reportexec.com Phone: 414.304.8500 Fax: 414.304.8570

Your Reports | In Your Inbox | On Your Schedule

Our Admin reporting module allows you to choose from a library of canned reports, or create your own report settings to generate the statistics that matter to you.

After you've customized your report settings, you can easily save the report for further use, or allow your report to automatically run and distribute. Just specify an interval (daily, weekly, monthly, etc.) for your report to generate automatically and enter your desired list of email recipients. Voila! Your reports show up in your inbox on your schedule—without any additional effort on your part.



25 MODULES. 1 PLATFORM.

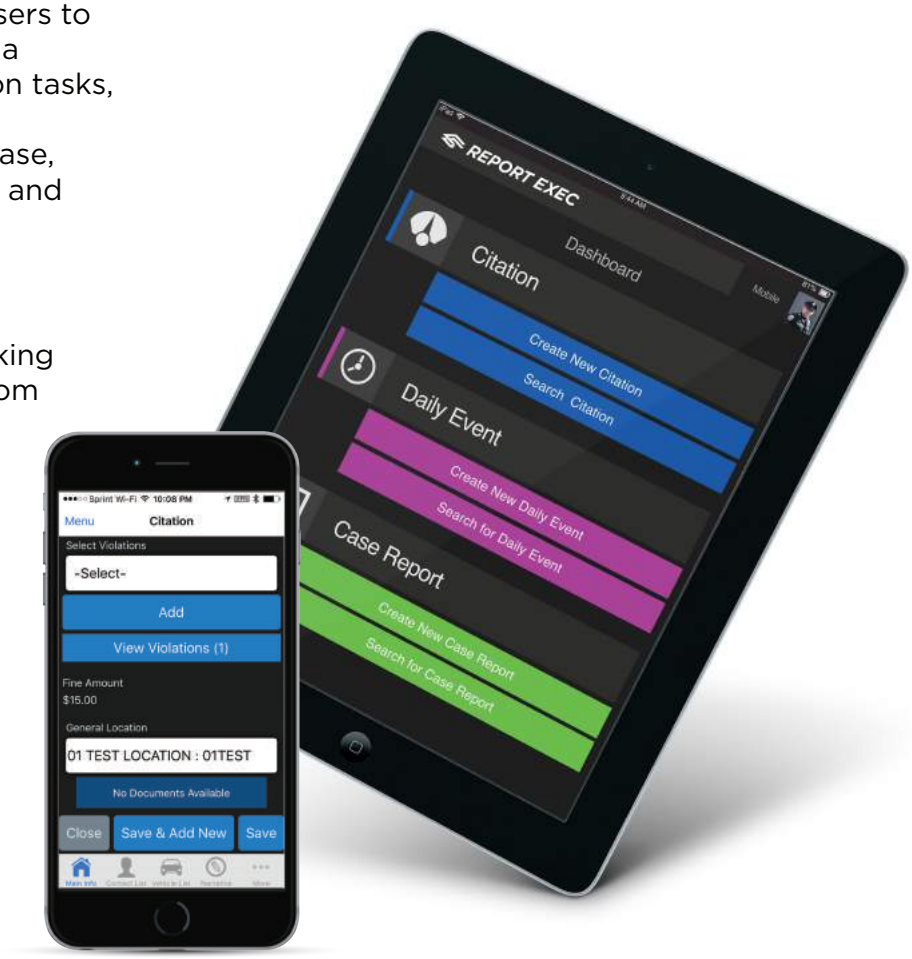
When you get Report Exec, you get it all. One easy-to-use application packs the punch of dozens. That means every file, every report, and every message is stored in one secure, searchable database. Your team only needs to learn one platform, and you've got audit trails for every action performed in the Report Exec.

Working in one platform isn't just easier for the staff members that use Report Exec daily; it also creates a robust, dynamic database. For example, every contact entered into Report Exec is stored in the database, and every interaction they have with your staff is saved in their history. Users can easily view contacts' history, and even create pop up notifications to make note of people who require assistance, have been combative in the past, or should not be permitted on premise. The database also helps analysts make connections between seemingly unrelated circumstances or events to identify root causes of incidents and assist in prevention efforts.

REPORT EXEC MOBILE

For iOS & Android

Report Exec Mobile allows Report Exec users to work efficiently while they are away from a computer. Designed to streamline common tasks, the application allows users to access information from their Report Exec database, capture digital media from the field, issue and print citations, and track daily events.



Efficient Citations
Issue citations while patrolling parking areas, and print citations direcly from the mobile application.

Daily Event Log
Keep daily event logs up to date by entering log information as it occurs while in the field.

Case Reports
Quickly record case report information from the field while details are fresh.

Search
Search daily event logs, citations, vehicles, contacts, and more efficiently.

Capture
Report Exec Mobile is designed for quick data capture. Use built-in cameras on a mobile device to capture digital images and videos to attach to citations, event logs and reports.

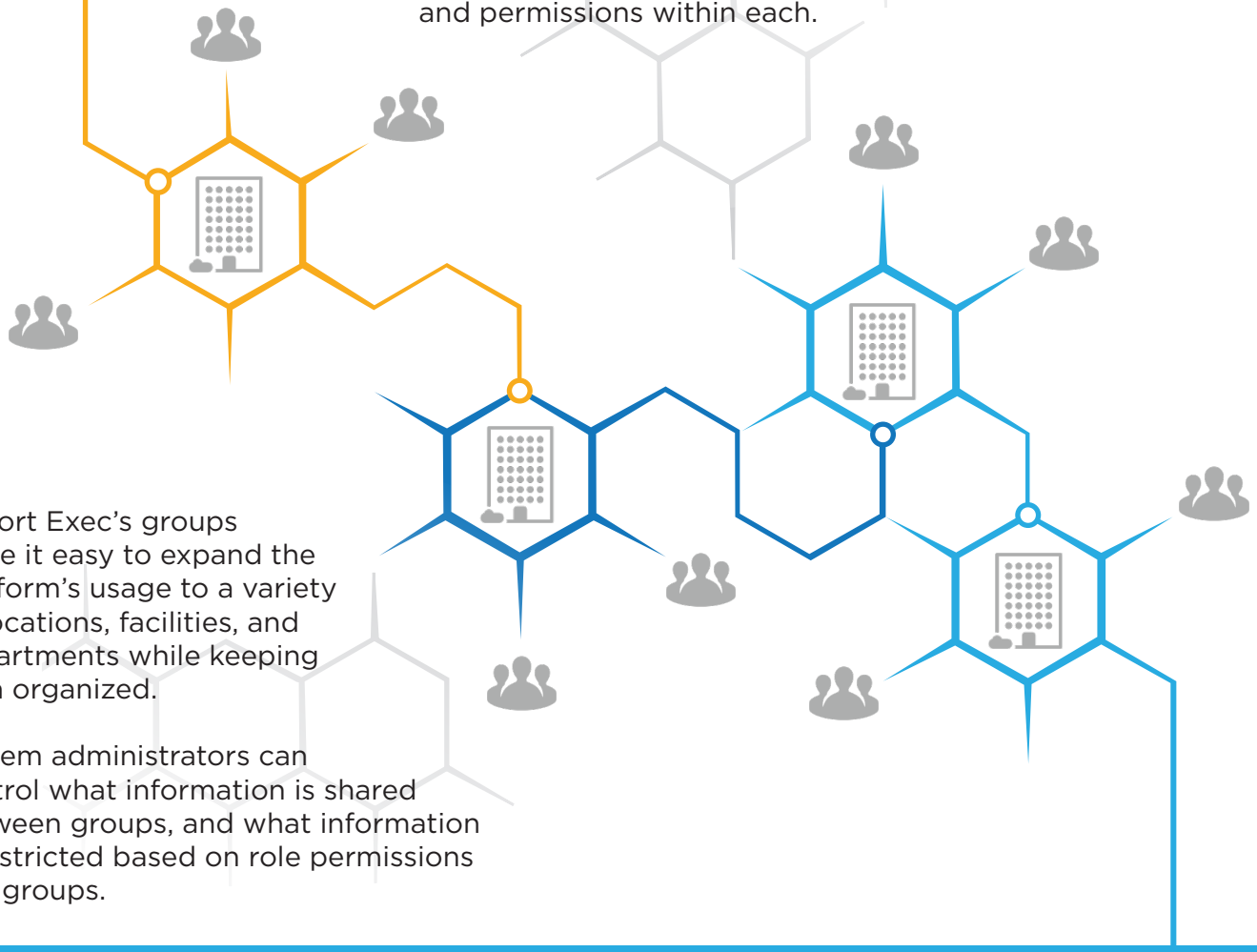
Create
Report Exec Mobile reduces data entry time with easy layouts and intuitive workflows. Record daily events in real time, issue citations on the go, and enter case report details in a flash.

Connect
Report Exec Mobile makes it easy to access your database no matter where you are. With search capabilities and better information in the field, you can make better decisions.

BUILT TO SCALE

With unlimited groups, Report Exec is ideal for growing organizations.

Each group creates its own reports while contributing to a central database of valuable information. Some users may belong to more than one group, and can have distinct roles and permissions within each.



Report Exec's groups make it easy to expand the platform's usage to a variety of locations, facilities, and departments while keeping data organized.

System administrators can control what information is shared between groups, and what information is restricted based on role permissions and groups.

The possibilities are endless.

Multi-national corporations use Report Exec to manage security across diverse locations. Users at each location have access to data that is relevant to their operations, while corporate headquarters can compare data from any and all locations. Many companies use groups to expand program use to Risk Management, Human Resources, and Facilities Management departments.

Need another group? No problem.

Unlimited groups are included with Report Exec.

THE BOTTOM LINE

Improved efficiency. Serious ROI.

Report Exec saves time for security departments as well as administrators by automating complex, time-consuming processes. Time and again, users that had previously employed homegrown systems for incident reporting and records management can't believe how easy is it to capture information and compile reports within the Report Exec system.

The software enhances accuracy while significantly reducing the time it takes to enter information and generate reports. This boost in efficiency can reduce labor costs and improve compliance. Most importantly, an efficient reporting process helps security officers spend more time doing what they do best: protecting your organization.

Every organization is different, but some estimate that Report Exec has reduced the time spent on paperwork by 50%. Our streamlined review processes slash the time for reviewing and correcting reports; some organizations report a 90% reduction in time from submission to approval. In addition to time saved, users report an overall higher report quality. The level of data captured in Report Exec is far superior to traditional methods, and the program makes connections between data points without requiring additional effort on the part of the user.

Sample Report Exec ROI Analysis	
Average Officer Salary and Benefits	$48,356
% of time spent on paperwork	10%
Paperwork cost	$4,836
Average reduction in time required for paperwork	50%
Cost savings per officer	$2,418
Annual subscription cost per officer	$1,380
Net cost savings	$1,038
ROI	75%

Departmental Budgeting & Performance

It can be difficult to show ROI for security spending, since a conventional "return" can't be provided. The benefit is in preventing loss of revenue: damaged property, lawsuits, injuries, or damaged reputation. Putting a price tag on prevention isn't easy. With Report Exec, however, it's becoming easier to see exactly what security expenditures provide. Security departments can use the program to effectively measure and record activities, justifying budget requests and ensuring funds are spent responsibly. Report Exec makes it easy to run departmental audits that are immensely useful when it comes to demonstrating demand for services provided, measuring the impact of the department, comparing departmental workloads and response times to national standards, projecting security expenditures based on needs, and even conducting individual performance reviews.

A TRUSTED SOLUTION

Report Exec is a provider of choice for over 1,100 organizations worldwide. For 22 years, we've been delivering premium software with excellent customer service and using customer feedback to guide our software development process. Report Exec is growing quickly and expanding our product offerings as well as our customer base. Below is a small sample of our satisfied clients.

The Security Management Support Team

President, William H. Nesbitt, CPP & Certified CPTED Practitioner

William H. Nesbitt, CPP is a Security Consultant with more than 38 years of diverse security experience. His healthcare experience began as **Corpsman in the United States Navy** stationed at the U.S. Navy Hospital in Philadelphia. Bill is a **Certified Protection Professional (CPP)** having sat for the first CPP Examination in 1978. He is President of **Security Management Services International, Inc**. (dba **SMSI Inc.),** a security consulting firm that provides services such as comprehensive security assessments, security design, training, security awareness programs and security management support services. **SMSI Inc.** provides these services to a wide array of clientele such as manufacturing facilities, shopping malls, hospitals, high-rise buildings and bio-tech companies, to name a few.

Bill also is a court-certified security expert and has been retained in over 400 security related lawsuits covering 40 states. His cases have included homicides, assaults, infant abductions, larceny, cargo theft, warehouse burglaries, sexual assaults, infant abductions and elder abuse. He has also handled intentional tort cases such as false arrest, false imprisonment and excessive use of force. Every litigation provides mitigation lessons.

Bill is a member of ASIS International's Healthcare Security Council, IAHSS, ASHRM, SCAHRM, and ACHE.

Bill is also a **Certified CPTED (Crime Prevention Through Environmental Design) Practitioner.** The application of **CPTED** design principals is probably one of the most cost efficient strategies one can apply to a broad range of security challenges (That is why **CPTED** is at Level One on the **Security Solution Hierarchy)**.

Bill frequently shares his experience as a speaker on a wide array of security topics. Most recently Bill Nesbitt has joined the ranks of approximately 150 security professionals, who in the last five years have completed the **ASIS International's Management Course for Security Executives at the Wharton School at the University of Pennsylvania.**

Bill has also served as an instructor for the Criminal Justice Institute at the University of Wisconsin, Milwaukee (1994).

Bill may be reached at **805-499-3800** or at bill@smsiinc.com

FLORIDA ATLANTIC UNIVERSITY

INSTITUTE FOR DESIGN AND CONSTRUCTION

School of Architecture

awards this

Certificate of Completion

to

William Nesbitt

for participation in the 40-hour CPTED Practitioner Seminar:

Crime Prevention Through Environmental Design

30 AIA LU/HSW/SD credits and 4 FAU CEUs have been awarded
on this thirteenth day of December, Two Thousand and Thirteen
in Fort Lauderdale, Florida

CONTINUING EDUCATION AIA

Deirdre Hardy, AIA
Professor and Director, School of Architecture

Randall I. Atlas, Ph.D., AIA, CPP
Instructor

Leigh McFarland, Ph.D.
Director, Institute for Design and Construction

Ronald Lander, CPP, CMAS, CHEPS, PSM

Ronald (Ron) Lander, Certified Protection Professional, Certified Master Anti-Terrorist Specialist and Physical Security Manager is a retired decorated Sergeant with 23 years on the **Los Angeles County Sheriff's Department**. Ron has been Chief Technology Officer (CTO) for **Security Management Services International, Inc.** (SMSI) for over twelve years. Ron is also owner of Ultrasafe Security Specialists, an integration and consulting enterprise in Southern California.

Ron's law enforcement experience includes burglary, property and high technology crime investigations, supervision in the Juvenile Investigations Bureau, the Undersheriff's Office and Data Systems Bureau. Ron continues in his role of supporting law enforcement by consulting on technology issues for law enforcement agencies throughout the United States. His combined experience in IT, security and law enforcement has been invaluable in many scenarios throughout the country.

In 2006, Ultrasafe Security, won the **"Sammy"** Award for the "Best Integrated Installation" in Northern America. There were over 100 entries. This coveted award is considered the "Oscar" of the security industry and the installation was featured in the July 2006 issue of Security Sales and Integration magazine. Ultrasafe was also runner up for the 2010 award.

In September 2008, Ron was the first recipient of the **Roy N. Bordes** Council Member "Award of Excellence" for his over 14 years of volunteer contributions to ASIS Councils and his countless lectures throughout the world on the behalf of ASIS International and the security community.

Ron became Board Certified in Security Management (CPP) in 1994. He became certified as a Master Antiterrorist Specialist (CMAS) in 2004, Physical Security Manager (PSM) in 2014 and Healthcare Emergency Management Specialist (CHEPS) in 2016. Recently spent two three-year terms as an ASIS Council Vice President (CVP), where he managed several groups of Subject Matter Experts in several disciplines.

Ron was also one of only five recent recipients worldwide of the **ASIS Presidential Award of Merit** and the recipient of the Region 3 (West Coast) "Outstanding CPP" Award for his "superior work" in "Protection of Sensitive Information."

In 2014, Mr. Lander was selected as a **"George Weinstock Jr. Lifetime Achievement Award**" recipient. He was the 17th annual recipient of this prestigious award, bestowed by the California Alarm Association (CAA). **Ron is the only member of the security industry who has won the "Bordes", Weinstock" and "Sammy" awards.**

Ron is now a member of the ASIS Risk, Threat and Vulnerability Assessment Training team. He and his fellow trainers will travel around the country, annually, teaching fellow security professionals the art and science of conducting Assessments. He was also a member of the Security Assessment Standards working group and is now active in the group creating a standard for Security Awareness.

In a **Security Management Support** role, **Ron** will ensure that **SMS** clients are neither oversold nor undersold when applying security technology, such as video surveillance systems, alarm system, access control system as well as visitor pass systems, infant security systems and asset protection. His knowledge of the use of security technology and the meaningful application of that technology is second to none.

Ron Lander has double-barreled experience, having been involved concurrently with security installations and law enforcement early in his career. After retiring as a decorated sergeant with over 23 years on the Los Angeles County Sheriff' Department, he was able to expand his security technology experience exponentially.
As a security integrator, Ron has had experience with the entire array of technology from custom access control systems and design to detailed high profile video surveillance projects. He has also been involved in the evaluation and judging of emerging technologies. He has conducted nearly 100 security and risk vulnerability assessments and now teaches the subject throughout the country.
Ron's award-winning career of over thirty-five years includes certifications in security management, healthcare emergency management, physical security management and terrorism preparation and prevention.

Because Ron is well integrated into the law enforcement brotherhood, he is often an asset to the clients we serve.

Anjanette Hebert, CHPA

Ms. Hebert is a healthcare emergency preparedness, security and safety professional with nearly 30 years of experience as a Healthcare Security Manager. She has served hospitals and the Emergency Medical Services community at state and federal levels. Ms. Hebert is also **a Certified Healthcare Emergency Professional and a Certified Healthcare Protection Administrator (CHPA). Ms. Hebert** Recently retired from a large tertiary hospital.

Anjanette served **as Director of Security, Safety and Emergency Preparedness** for over **28** years along with additional oversight of Parking, Valet Services, PBX, Courier Services and Patient Van Services. Ms. Hebert served as Environment of Care Committee Chair, general Safety Officer, and Emergency Manager responsible for planning, training and implementation of emergency plans, drill and exercise development, implementation and evaluation and development of the patient decontamination team.

She was directly responsible for ensuring compliance with and maintaining documentation for TJC, CMS, OSHA and other relevant standards in all operations related to emergency preparedness, security and general safety. Ms. Hebert also served in a consultative role in these areas to six additional entities within the health system. In 2002, Ms. Hebert assumed the inaugural role of Emergency Preparedness Healthcare Coalition Lead for Region 4 in Louisiana, initiating the process of building a coalition that today consists of more than 40 entities including acute care hospitals, sub-acute hospitals, specialty hospitals, public health, EMS, and various other healthcare related entities.

Ms. Hebert holds a Bachelor of Criminal Justice degree and the distinction of Certified Healthcare Security Administrator and Certified Healthcare Emergency Planner. Because Ms. Hebert has spent most of her career well ensconced within the healthcare culture, she is readily accepted as a peer.

Obviously, Ms. Hebert has a great deal of experience in managing a large in-house security operation. She understands dealing with security vendors from the other side of the desk. She also understands that security methodologies, to be effective, must be driven by specific needs.