### Tuesday, April 14

<table>
<thead>
<tr>
<th>Time</th>
<th>Title</th>
<th>Track</th>
<th>Room</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:00 – 10:00 AM</td>
<td>Customizing Your Sales Action Plan</td>
<td>Workshops</td>
<td>302</td>
</tr>
<tr>
<td>8:30 AM – 12:30 PM</td>
<td>IAPSC Successful Security Consulting Seminar (Offered as a comprehensive program. Sessions cannot be taken individually.)</td>
<td>IAPSC Seminar</td>
<td>307</td>
</tr>
<tr>
<td>8:30 AM – 10:00 AM</td>
<td>The Business of Security Consulting From Consulting 101 to Becoming a Certified Security Consultant</td>
<td>Workshops</td>
<td>302</td>
</tr>
<tr>
<td>8:30 AM – 10:00 AM</td>
<td>Successful Security Consulting Introduction and Overview</td>
<td>Workshops</td>
<td>302</td>
</tr>
<tr>
<td>8:30 AM – 10:00 AM</td>
<td>Preparing a Responsive, High-Impact Consultant's Report</td>
<td>Workshops</td>
<td>302</td>
</tr>
<tr>
<td>8:30 AM – 10:00 AM</td>
<td>Proposing Security Consulting Services and Hiring a Security Consultant</td>
<td>Workshops</td>
<td>302</td>
</tr>
<tr>
<td>8:30 AM – 10:00 AM</td>
<td>Executing and Completing the Consulting Assignment</td>
<td>Workshops</td>
<td>302</td>
</tr>
<tr>
<td>8:30 AM – 10:00 AM</td>
<td>Extended Consulting Services: Designing and Implementing Integrated Management and Technical Solutions</td>
<td>Workshops</td>
<td>302</td>
</tr>
<tr>
<td>8:30 AM – 10:00 AM</td>
<td>Offering and Delivering Convergence Consulting Services: A Holistic Security Approach to Logical and Physical Security Integration</td>
<td>Workshops</td>
<td>302</td>
</tr>
<tr>
<td>8:30 – 10:00 AM</td>
<td>Security Planner Planning Your Roadmap to Success</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
<tr>
<td>8:30 – 10:00 AM</td>
<td>To Have or To Hire: The Advancement of IT Skills in the Physical Security Space</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
<tr>
<td>8:30 – 11:55 AM</td>
<td>Leveraging Risk Assessments to Improve and Raise Funding for Your Security Program</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
<tr>
<td>11:30 AM – 12:30 PM</td>
<td>Off-Broad-Based Security: “Right-Size” Your Security Program to Optimize Manpower and Budget</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
<tr>
<td>1:30 – 2:30 PM</td>
<td>Creating and Sustaining Value: The Scorecard for Selecting and Managing Your Services Team</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
<tr>
<td>1:30 – 3:30 PM</td>
<td>Troubleshooting Network Video</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
<tr>
<td>1:30 – 3:30 PM</td>
<td>Stand Down From the Competition</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
<tr>
<td>2:45 – 3:45 PM</td>
<td>The Forum for Creative Security Solutions</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
<tr>
<td>2:45 – 3:45 PM</td>
<td>Finding Danger From Within: Developing an Insider Threat Program</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
<tr>
<td>4:00 – 5:00 PM</td>
<td>Protecting the Protections: Cyber Hygiene for Physical Security</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
<tr>
<td>4:00 – 5:00 PM</td>
<td>Collaborative Best Practices for Next Generation Security Leaders</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
</tbody>
</table>

### Wednesday, April 15

<table>
<thead>
<tr>
<th>Time</th>
<th>Title</th>
<th>Track</th>
<th>Room</th>
</tr>
</thead>
<tbody>
<tr>
<td>7:30 – 8:30 AM</td>
<td>A Knowledgable &amp; Trustworthy 5th Generation Incident Commander</td>
<td>Dealer, Installer, Integrator</td>
<td>302</td>
</tr>
<tr>
<td>7:30 – 8:30 AM</td>
<td>Evaluating New Technologies and Growth Opportunities in the Access Control Video Surveillance &amp; Smart Home Industries</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
<tr>
<td>7:30 – 8:30 AM</td>
<td>Campus Police Investigation: How to Use CCTVs to Solve Crimes and Increase Your Effectiveness</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
<tr>
<td>7:30 – 8:30 AM</td>
<td>How to a Life Cycle Management Program Can Optimize Security Systems Performance</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
<tr>
<td>7:30 – 8:30 AM</td>
<td>How to Defend Law Enforcement Identification and Detection Capabilities through Smartphone Technology and Collaboration</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
<tr>
<td>8:00 – 9:00 AM</td>
<td>Taking Management Best Practices for the Security Industry</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
<tr>
<td>10:00 – 11:00 AM</td>
<td>The Seven Deadly Sins of Alarm Contrac- Common Errors and How to Correct Them</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
<tr>
<td>10:00 – 11:00 AM</td>
<td>Security Power Provisioning—Ensuring Operational Integrity</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
<tr>
<td>10:00 – 11:00 AM</td>
<td>Active Shooter and Workplace Violence It Can't Happen Here!</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
<tr>
<td>10:00 – 11:00 AM</td>
<td>The Evolving Cybersecurity Perimeter</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
<tr>
<td>10:00 – 11:00 AM</td>
<td>Case Study: Integrating Chemical Detection, CCTV and Access Control for Enhanced Public Safety</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
<tr>
<td>10:00 AM – 12:15 PM</td>
<td>PPWINVideo/Veriféd Alarms Training, Course I</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
<tr>
<td>11:15 AM – 12:15 PM</td>
<td>Welcome to Social Spaces: The Era of Social/Access Management</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
<tr>
<td>11:15 AM – 12:15 PM</td>
<td>University Improves Access Control in Residence Hall: What Businesses and Institutions Can Learn</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
<tr>
<td>12:30 – 1:30 PM</td>
<td>How To Do, Design, Package and Sell Service Agreements</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
<tr>
<td>12:30 – 1:30 PM</td>
<td>Adapting Mobile Credentials into Your Access Control Infrastructure</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
<tr>
<td>12:30 – 1:30 PM</td>
<td>Understanding Your CID: A Primer for Security and IT Rotations</td>
<td>Dealer, Installer, Integrator</td>
<td>304</td>
</tr>
<tr>
<td>12:30 – 2:00 PM</td>
<td>The Israeli Approach to Prevention School Security &amp; Safety 309</td>
<td>Dealer, Installer, Integrator</td>
<td>306</td>
</tr>
<tr>
<td>12:30 – 2:00 PM</td>
<td>Security Operation Centers: Build Your Own or Virtualize or Both</td>
<td>Dealer, Installer, Integrator</td>
<td>306</td>
</tr>
<tr>
<td>1:45 – 2:45 PM</td>
<td>Goshen Recognition Analytics: Delivering Actionable Information to Law Enforcement and First Responders</td>
<td>Dealer, Installer, Integrator</td>
<td>306</td>
</tr>
<tr>
<td>2:15 – 3:15 PM</td>
<td>Ready or Not...Mass Notification and Emergency Communications Are here to Stay</td>
<td>Dealer, Installer, Integrator</td>
<td>306</td>
</tr>
</tbody>
</table>

### SPECIAL THANKS TO OUR GENEROUS SPONSOR:

**SIA Education@ISC West offers various registration packages. See page 25 for more information or visit [http://www.iscwest.com/Education/Pricing/](http://www.iscwest.com/Education/Pricing/).**
# Sessions-at-a-Glance

## Thursday, April 16

### Time | Title | Room
--- | --- | ---
**8:45 – 9:45 AM** | The Internet of Things: The Promise for the Security Industry | Signature Series 701
**7:30 – 8:30 AM** | Video Surveillance Trends: Adapt or Risk Obsolescence | Physical Security 304
**11:15 AM – 12:15 PM** | Detecting Theft in the Self-Checkout | Video Surveillance 309
**7:30 – 8:30 AM** | Beyond the Buzz: A Balanced Look into the Future of Physical Security | Physical Security 304
**7:30 – 8:30 AM** | Making the Most of Big Data | Signature Series 701
**7:30 – 8:30 AM** | Stop Issuing Secure Credentials to Imposters | Access & ID Management 302
**7:30 – 8:30 AM** | The Fast Lane for Healthcare Security Leadership Success | Physical Security 304
**8:45 – 10:00 AM** | Protecting your Intellectual Property and Corporate Data While Traveling | Physical Security 304
**10:00 – 11:00 AM** | Getting the Most Out of Biometric Technology: Reduce Costs, Improve Processes and Boost Confidence | Access & ID Management 302
**10:00 – 11:00 AM** | Connecting Your Video System to the Internet: Mitigating Your Security Vulnerabilities and Threats | Video Surveillance 309
**10:00 – 11:00 AM** | The Fast Lane for Healthcare Security Leadership Success | Physical Security 304
**10:00 – 11:00 AM** | Protecting Your Intellectual Property and Corporate Data While Traveling | Next Generation Security 307
**10:45 – 11:15 AM** | Case Study: Lessons from the $1B San Diego Airport Design-Build Program | Physical Security 304
**11:15 AM – 12:15 PM** | Physical Security | Physical Security 304
**11:15 AM – 12:15 PM** | Next Generation Security | Next Generation Security 307
**12:30 – 1:30 PM** | You Own the Door, So Don’t Leave Dollars at the Threshold! | Access & ID Management 302
**12:30 – 1:30 PM** | Security Operations Centers: Providing the “Last Mile” | Physical Security 304
**12:30 – 1:30 PM** | Mobile and Connected Commerce: A Game Changer or Security Nightmare? | Next Generation Security 307
**1:45 – 3:00 PM** | The Command Center Experience: From Design to PSSM | Signature Series 701

---

### SPECIAL PRICING

SIA Education@ISC West offers various registration packages. See page 25 for more information or visit [http://www.iscwest.com/Education/Pricing/](http://www.iscwest.com/Education/Pricing/).

---

### Tuesday, April 14

#### IAPSC: (International Association of Professional Security Consultants)

**Tuesday, April 14 • 8:30 AM – 5:00 PM**

**IAPSC Successful Security Consulting Seminar**

The IAPSC Successful Security Consulting Seminar is offered as a comprehensive program. Sessions cannot be taken individually.

**IAPSC SESSION 1: Successful Security Consulting: Introduction and Overview**

8:30 – 8:45 AM

The course introduction summarizes course offerings, introduces key faculty and explains how each element of the course applies to a variety of security consulting engagements. Participants will be asked to summarize their own course objectives and describe what they expect to learn and achieve. Lastly, the introduction will emphasize practical, hands-on information on the business aspects and execution of security consulting that can save you time, money and confusion when completing a security consulting assignment or starting a new practice.

**IAPSC SESSION 2: The Business of Security Consulting: From Consulting 101 to Becoming a Certified Security Consultant**

8:45 – 10:00 AM

In The Business of Security Consulting, participants learn the essential truths for success as a security consultant; how to build a practice; and how to add value to a clients’ operation through key consulting specialties, like Technical and Management Consulting, Forensics and IT Security Consulting. Learn how to develop and implement a realistic business plan that focuses on building a trust relationship with service recipients, the security consultant’s role in an organization, and implementing one of the five key consulting phases.

Special emphasis is put on the Marketing aspects of building a successful security consulting practice, how to make your business “fit” the desired marketplace in which your expert services will be sold, how to use your professional network, and how to develop and hone specialized marketing and communications skills for a successful consulting engagement. Specific challenges and tips for dealing with services marketing or sales implementation problems will be shared. Those include the best ways to position your business and services, deal with competition and target a specific industry.

**IAPSC SESSION 3: The Financial and Administrative Aspects of Security Consulting**

10:15 – 11:00 AM

Learn the essential administrative and accountancy aspects of the consultant’s practice and how to administer the practice as a business on a daily basis. This session addresses the financial aspects of starting and operating as an individual consulting entity, including business financial planning; setting up the legal corporate entity; documenting your specific consulting services; meeting insurance requirements; setting up your office, including its accounting, budgeting and human resource functions; performing the scope of work within budget; invoicing and collecting payment; and establishing performance metrics. Additionally, participants learn how to set a reasonable bill rate and cost basis hourly rate, including your own and any subcontractor compensation, expenses and billable hours.

**IAPSC SESSION 4: Proposing Security Consulting Services and Hiring a Security Consultant**

11:00 AM – 12:00 PM

Identifying consulting opportunities, developing winning proposals and beating out the competition are the primary focus of this session. Additionally, participants explore the critical elements of hiring a security consultant to address the short- and long-term security needs of an organization based on whether limited or complex security requirements and expertise are necessary. Particular emphasis is placed on how to develop and land sole source vs. competitive opportunities; how and when to prepare competitive written proposals; how to fully and completely respond to a bid; and how to win proposals, and beating out the competition are the primary focus of this session.

**IAPSC SESSION 5: Executing and Completing the Consulting Assignment**

1:00 – 2:00 PM

In this session, participants learn how to successfully complete the consulting assignment and further the trust relationship, such that the client or end-user is sold on and re-uses the consultant’s value services repeatedly. The types of essential consulting skills (technical, interpersonal and consulting) are addressed in the four key phases of consulting: contracting, discovery, feedback and decision. The goals and objectives of...
of the consultant in an engagement are taught in terms of identifying problems and solutions, and engaging in actions that result in people or organizations managing themselves or doing things differently. Special emphasis is placed on how to develop and build influence over an individual, group or organization when the consultant typically has no direct power or resources to make changes or implement programs internal to that organization.

Participants learn how to survey existing security programs or systems and conduct security audits in which operations are measured against specific documentation, such as standards, guidelines and regulations. Various phases of the security assessment are explored, including how to conduct asset, threat, vulnerability, risk and requirements analyses. Participants are introduced to frequently-used automated assessment tools and how the results of these assessments should be included in the consulting assignment.

IAPSC SESSION 6: Preparing a Responsive, High-Impact Consultant’s Report
2:00 – 3:00 PM
In this practical session, participants learn about and receive examples of the types of written reports and report formats typically prepared and submitted by security consultants: Security Assessment Report, Design Concept Report, System Design and Assessment Phase Report, Architectural Project Phase Reports, Design Specifications and Drawings, and Forensic Reports. Specific content, outlines and examples of each are discussed and presented.

IAPSC SESSION 7: Extended Consulting Services: Designing and Implementing Integrated Management and Technical Solutions
3:15 – 4:15 PM
Technical security consultants assist clients in determining how to accurately identify technical solutions and integrate them into overall technical security systems culminating in a comprehensive, integrated security program for cost effectiveness and risk reduction. In this session, participants delve into the security system design and implementation process by first identifying the four major phases of design: Schematic Design, Preliminary Design, Detailed Design and Construction Documents. Experienced designers guide participants through the technical pitfalls of design and construction, emphasizing the design process “safety nets” that are in place as the process moves from one gate to the next. Participants learn how to solicit owner and other stakeholder input; determine design requirements and constraints; avoid costly change orders; enhance their technical reputation; and deliver value to the client by implementing a proven process by acting as a change agent, security expert, systems engineer or architect, all in one technical consulting assignment.

IAPSC SESSION 8: Offering and Delivering Convergence Consulting Services: A Holistic Security Approach to Logical and Physical Security Integration
4:15 – 4:45 PM
This session explores Convergence Consulting, a holistic view of delivering physical and logical security consulting services, and how it is fast becoming the preferred approach for more progressive organizations with a Chief Security Officer (CSO) who handles both physical and logical requirements. Learn how the emergence of networks and technology integration has resulted in quantum shifts in the security industry and how security services are delivered within a particular organization. The session covers how security consulting is now split between physical and logical security, and how the issue of organizational convergence of security (physical & logical) is more an organizational than a technical phenomenon. Learn how certain types of organizations can benefit from convergence consulting services and how the key aspects of risk management and control are addressed in the paradigm. Participants receive a model for Convergence Consulting that outlines the benefits of assuming a holistic view of an organization’s risks and security elements under one set of requirements.

IAPSC SESSION 9: Summary & Seminar Wrap-up
4:45 – 5:00 PM
Learn how to identify, rank and plot various attributes involved in the sales process, aligning them to create effective sales maps or action plans. Working in small teams, participants create a Sales Action Matrix for a real company exhibiting at ISC West. Some teams will present their plans and field questions from the audience to simulate the process. This technique can be used to analyze your competitors, too.

Learning Objectives
1. Achieve sustainable sales growth by developing an effective and actionable plan based on an empirical process that assigns numerical value to various attributes.
2. Assign “attribute values” related to your product, sales team, target market and competition.
3. Develop a Sales Action Matrix by analyzing product, marketing, sales strategy and channel strategy.

Tuesday, April 14 • 10:30 AM – 12:30 PM
Sales Estimating for Sales, Operations and Your Customer’s Success
The estimating process can be daunting in today’s world of changing demands, technologies and project complexities. The Sales team projects the success of the job each time a proposal is accepted by a customer. Success is based on rock-solid estimating practices—getting it right when specifying the parts, labor, cost items and recurring monthly revenue at the right pricing for each job. From there, Operations has to deliver! Join us for a workshop focused on best practices in the sales and estimating process for the purpose of enhancing gross profit, providing an excellent “hand-off” to Operations and winning the customer relationships most important to your organization.

Learning Objectives
1. Achieve sustainable sales growth by developing an effective and actionable plan based on an empirical process that assigns numerical value to various attributes.
2. Assign “attribute values” related to your product, sales team, target market and competition.
3. Develop a Sales Action Matrix by analyzing product, marketing, sales strategy and channel strategy.

Tuesday, April 14 • 8:00 – 10:00 AM
Customizing Your Sales Action Plan
Identifying the most compelling attributes of a salesperson, product, channel or marketing strategy are key to sales success. In this workshop, participants learn a technique that assigns numerical value to various attributes that can then be aligned to create planning documents, such as sales action plans or competitive matrices. This workshop is ideal for sales people and sales managers at any level of development who want to systemize their sales planning into an effective and actionable document.

Learning Objectives
1. Establish consistent methods and practices for creating sales estimates.
2. Learn how to “think the job” to estimate and record labor types and time required for your projects.
3. Identify key words and clauses requiring attention when answering RFPs and reviewing project drawings, contracts and other documents.
4. Write excellent scopes of work.
5. Take home 5 best practices to improve sales success within your organization.
In this interactive Learning Lab, participants learn to build and troubleshoot an IP network capable of transporting IP video surveillance securely and reliably, obtain hands-on experiences for building on network architectures, and determine how to scale these for both small and large deployments. Additionally, participants gain an introduction to basic networking terms and concepts. Security integrators, consultants, practitioners and specifiers learn about deploying networks, how they affect the end-user experience, recognize how to ask the correct questions when dealing with the IT/networking team as it relates to deployment for surveillance installations, and gain confidence deploying a basic network capable of transporting IP video surveillance traffic.

**Learning Objectives**

1. Define basic networking terms and basics of IP networks, including Local Area Network (LAN) and Wide Area Network (WAN), the OSI model, and types of network devices.
2. Describe how digital video surveillance (or other type of data packets) traverse from source to target in an IP network.
3. Configure a basic network from layers 1 - 3 of the OSI layer.

**Tuesday, April 14 • 8:30 AM – 10:00 AM**

**To Have or To Hire: The Advancement of IT Skills in the Physical Security Space**

As IP-based security technologies and IT-centric systems become more prevalent in today's physical security solution set, IT skills sets become increasingly more critical to have or to hire. Is your organization prepared to meet the demand? Join us as integrators and manufacturers weigh in on the changes taking place that affect operations, recruiting, partnering, outsourcing and go-to-market strategies.

**Learning Objectives**

1. Define the common IT skill sets employed to sell, support and service IT-centric solutions.
2. Examine the pros and cons of recruiting, outsourcing and partnering approaches to scale your IT skilled workforce.
3. Devise a plan to operationalize your migration to a more IT-savvy approach.

**Tuesday, April 14 • 11:30 AM – 12:30 PM**

**Get Off My Cloud! Best Practices in Securing the Cloud**

Cloud-based services are more robust and commonplace in security applications than ever before; however, security for the cloud remains a concern. Corporations are blamed for poor security, hackers with malicious intent are a given threat and lax password practices on the part of users make cloud security a tough case to crack. This must-attend session is designed for anyone interested in adopting a more secure cloud strategy for his/her organization. Come hear manufacturers discuss their efforts to provide better security for cloud-based solutions.

Learning Objectives:

1. Discuss the end-to-end architecture of digital video surveillance architecture and how it differs from CCTV.
2. Greatly reduce downtime of mission critical applications and equipment.
3. Gain real-world shortcuts for bringing systems back to life.

**Tuesday, April 14 • 1:30 – 3:30 PM**

**Troubleshooting Network Video**

This Learning Lab features an extensive step-by-step four-dimensional view of all the components for a digital video surveillance system, including power (electrical); software (video management systems; PSM, networking); hardware (cameras network switches, radios); and communications (OSI layers, wireless, fiber). Participants gain insights on real-world video surveillance case studies and explore details of how to utilize troubleshooting charts to save time and money, and observe details on the complexity of the IP solutions currently being implemented by traditional CCTV hardware-driven integrators and architects.

**Learning Objectives**

1. Investigate methods employed by manufacturers to improve security for cloud-based solutions.
2. Identify what works and what doesn’t in securing the cloud.
3. Adopt universal best practices for practitioners, service providers and manufacturers to work together to improve security for cloud-based services.

**Tuesday, April 14 • 1:30 – 2:30 PM**

**Open vs. Proprietary Platforms: On Which Should You Build Your Future?**

From proprietary to open solutions, what is the lifecycle expectation of a system platform and how do you decide which is the best system to use? Enterprise customers can’t afford to experiment with major platforms employed in their operations. How do you decide on which platform to standardize? Are you better off with open versus proprietary solutions? Can an enterprise customer ever benefit from an “early adopter” of technology? Join us to assess the pros and cons of open and proprietary platforms against your present and future business needs.

**Learning Objectives**

1. Assess the pros and cons of open versus proprietary platforms.
2. Catalog, analyze and classify your platform choices based on present and future business needs.
3. Identify ways to test if your manufacturer is designing for the future.

**Tuesday, April 14 • 2:45 – 3:45 PM**

**The Forum for Creative Security Solutions**

This session examines a series of customer case studies in which innovative and unconventional solutions were developed to solve uncommon problems. Starting with a statement of a unique real-life customer situation that defined a conventional approach, a panel of industry experts and session attendees are invited to offer potential solutions. The final resolution will then be revealed along with the supporting rationale and what was needed from the manufacturer or integrator to make it happen. Cases will be drawn from across the industry and will be selected to showcase truly innovative thinking and approaches by practicing security personnel.

**End-User Strategic Management**

**Tuesday, April 14 • 8:30 AM – 10:00 AM**

**Security Master Planning: Your Roadmap to Success**

In this session, experts demonstrate the value and process to develop a master plan for security that dovetails with the business master plan and/or corporate mission. Participants gain a roadmap from which future security projects and organizations are developed and/or managed in the organization. Learn about the justification and benefits from the activity methodology to produce a master plan, how to apply the strategy to both large and small entities, the elements of a security master plan, and the metrics used to evaluate and demonstrate the performance of the plan.

**Tuesday, April 14 • 1:45 – 2:45 PM**

**The Physical Security Space**

In this session, experts will demonstrate the value and process to develop a master plan for security that dovetails with the business master plan and/or corporate mission. Participants will gain a roadmap from which future security projects and organizations are developed and/or managed in the organization. Learn about the justification and benefits from the activity methodology to produce a master plan, how to apply the strategy to both large and small entities, the elements of a security master plan, and the metrics used to evaluate and demonstrate the performance of the plan.

**Learning Objectives**

1. Use real-life case studies to identify ways manufacturers and integrators respond to unusual customer challenges.
2. Compile a list of creative solution ideas with potential applications to difficult problems.
3. Explain what may be involved in truly meeting a customer need.

**Tuesday, April 14 • 4:00 – 5:00 PM**

**Protecting the Protectors: Cyber Hygiene for Physical Security**

Cyber security events are not entirely preventable, yet experts in the cyber security field suggest that a significant risk of cyber incursions could be substantially mitigated if enterprises engaged in good “cyber hygiene.” These best practices are often well-known, simple common sense approaches that should be a part of an enterprise culture. Learn how to reduce risk to your network and enterprise by identifying the most common sources of risk and exposure that can be prevented by effective cyber hygiene.

**Learning Objectives**

1. Define the term “cyber hygiene” and outline common best practices.
2. Identify the most commons sources of risk and exposure that can be prevented by good cyber hygiene.
3. Establish a priority of best next steps to implement good practices for cyber hygiene in order to reduce risk to the network and enterprise.

**Tuesday, April 14 • 2:45 – 3:45 PM**

**The Forum for Creative Security Solutions**

This session examines a series of customer case studies in which innovative and unconventional solutions were developed to solve uncommon problems. Starting with a statement of a unique real-life customer situation that defined a conventional approach, a panel of industry experts and session attendees are invited to offer potential solutions. The final resolution will then be revealed along with the supporting rationale and what was needed from the manufacturer or integrator to make it happen. Cases will be drawn from across the industry and will be selected to showcase truly innovative thinking and approaches by practicing security personnel.

**Learning Objectives**

1. Investigate methods employed by manufacturers to improve security for cloud-based solutions.
2. Identify what works and what doesn’t in securing the cloud.
3. Adopt universal best practices for practitioners, service providers and manufacturers to work together to improve security for cloud-based services.

**Tuesday, April 14 • 1:30 – 2:30 PM**

**Open vs. Proprietary Platforms: On Which Should You Build Your Future?**

From proprietary to open solutions, what is the lifecycle expectation of a system platform and how do you decide which is the best system to use? Enterprise customers can’t afford to experiment with major platforms employed in their operations. How do you decide on which platform to standardize? Are you better off with open versus proprietary solutions? Can an enterprise customer ever benefit from an “early adopter” of technology? Join us to assess the pros and cons of open and proprietary platforms against your present and future business needs.

**Learning Objectives**

1. Assess the pros and cons of open versus proprietary platforms.
2. Catalog, analyze and classify your platform choices based on present and future business needs.
3. Identify ways to test if your manufacturer is designing for the future.

**Tuesday, April 14 • 2:45 – 3:45 PM**

**The Forum for Creative Security Solutions**

This session examines a series of customer case studies in which innovative and unconventional solutions were developed to solve uncommon problems. Starting with a statement of a unique real-life customer situation that defined a conventional approach, a panel of industry experts and session attendees are invited to offer potential solutions. The final resolution will then be revealed along with the supporting rationale and what was needed from the manufacturer or integrator to make it happen. Cases will be drawn from across the industry and will be selected to showcase truly innovative thinking and approaches by practicing security personnel.

**Learning Objectives**

1. Investigate methods employed by manufacturers to improve security for cloud-based solutions.
2. Identify what works and what doesn’t in securing the cloud.
3. Adopt universal best practices for practitioners, service providers and manufacturers to work together to improve security for cloud-based services.

**Tuesday, April 14 • 1:30 – 2:30 PM**

**Open vs. Proprietary Platforms: On Which Should You Build Your Future?**

From proprietary to open solutions, what is the lifecycle expectation of a system platform and how do you decide which is the best system to use? Enterprise customers can’t afford to experiment with major platforms employed in their operations. How do you decide on which platform to standardize? Are you better off with open versus proprietary solutions? Can an enterprise customer ever benefit from an “early adopter” of technology? Join us to assess the pros and cons of open and proprietary platforms against your present and future business needs.

**Learning Objectives**

1. Assess the pros and cons of open versus proprietary platforms.
2. Catalog, analyze and classify your platform choices based on present and future business needs.
3. Identify ways to test if your manufacturer is designing for the future.
Learning Objectives
1. Identify corporate risks and connect them with security-specific risk.
2. Justify the benefits of the master plan to corporate management.
3. Develop metrics to evaluate the effectiveness of the master plan.

Tuesday, April 14 • 10:15 – 11:15 AM
Leveraging Risk Assessments to Improve and Raise Funding for Your Security Program

A properly conducted risk assessment is a tremendous resource when identifying opportunities for improvement and establishing baselines for key metrics within a security management program. However, the information is only valuable if appropriate action is taken to address the findings. Creating goals, generating a gap analysis and formulating a budget are challenges faced by many security directors today. Uncovering weaknesses while protecting your professional credibility can be a delicate balance. In this session, participants not only review expectations for a risk assessment and best practices in interpreting the information and solutions to common vulnerabilities, but also discuss proven methods for presenting the findings and proposing an improvement plan to executive management.

Learning Objectives
1. Prepare and provide a plan for a risk assessment.
2. Establish baseline performance metrics and key performance indicators.
3. Develop and present a budget for improvement to executive management.

Tuesday, April 14 • 11:30 AM – 12:30 PM
Effects-Based Security: “Right Size” Your Security Program to Optimize Manpower and Budget

Effects-based security (EBS) allows security directors and their companies to tailor their security systems to their threat and risk. There is no “one size fits all” solution in today’s threat environment. Security professionals often have difficulty quantifying their programs in terms of risk, cost and return on investment. EBS aids you in tailoring your risk program within realistic cost constraints and offers a risk reduction calculator to support program advocacy. It builds on a systems-based thinking approach supported by procedures and processes. Join us to learn how to implement EBS and how it can improve your security programs.

Learning Objectives
1. Assess how effects-based security can contribute to a logical and supportable security program tailored to your organization’s vulnerabilities and risk.
2. Conduct a risk assessment of your organization by measuring threats and vulnerabilities by using EBS to reduce risk.
3. Build a business case for EBS using a practical mix of technology, manpower and procedures tailored to your risk level.

Tuesday, April 14 • 1:30 – 2:30 PM
Creating and Sustaining Value: The Scorecard for Selecting and Managing Your Services Team

A next generation risk, resilience and security program relies on the competencies and capacities of a network of consultants and integrators. Increasingly, this network must function in collaboration with their client and with each other to fully optimize and leverage subject matter expertise. Is the industry ready to create a new way of evaluating service vendors? Are you optimizing and leveraging your consultants, integrators and service providers so that you are able to build and sustain a valuable security program? Join an expert panel as it identifies current vendor practices and emerging business models that are changing the definition of security management and the value proposition for security services.

Learning Objectives
1. Outline the key characteristics for choosing key consultants, architects, integrators, installation companies and vendors.
2. Identify the costs, metrics, disciplines and best practices essential to managing and leveraging a thriving security vendor network.
3. Develop a scorecard to rank your current ability to leverage and manage a team of service vendors.

Tuesday, April 14 • 2:45 – 3:45 PM
Finding Danger from Within: Developing an Insider Threat Program

From Brutus betraying Caesar to Bradley Manning and Edward Snowden, insider threats are an inevitable challenge to any organizational security program. The National Counterintelligence Executive lists insider threat as one of the top three greatest security challenges of today, alongside cyber threats and supply chain risk management. For the Nation’s cleared contractor community, 2015 welcomes new mandates to establish an insider threat program and designate an Insider Threat Awareness Officer, but many companies have not dealt with insider threats in a systematic way. This discussion provides corporate leaders and security managers with a roadmap for establishing an insider threat program, utilizing counterintelligence techniques already used at the nation’s cleared labs, military installation and defense companies. It provides guiding principles for program development, highlights legal landmines, addresses the formation of an insider threat working group, and walks you through the 10 steps to an effective insider threat program.

Learning Objectives
1. Define insider threats by type and examples.
2. Identify indicators and risk factors for insider threats.
3. Outline 10 steps to form an insider threat working group.
4. Identify compliance requirements and legal “landmines” when implementing an insider threat program.

Tuesday, April 14 • 4:00 – 5:00 PM
Collaborative Best Practices for Next Generation Security Leaders

Learn how to use thought leadership and build relationships with other security organizations to deliver better security services and solutions. In this session, a panel of industry leaders representing the Security Industry Association, the International Security Management Association and the Domestic Security Alliance Council outline the benefits of collaboration among security associations. Speakers address the advantages of maintaining relationships with other security organizations and the typical reasons for resistance. Through the lens of our panelists’ personal experience and real-world examples of external collaboration, learn how collaboration is strengthening the industry, shaping its future and affecting the next generation of security leaders.

Learning Objectives
1. Increase your use of traditional, non-traditional and social media tools and practices to identify talent for your organization.
2. Employ a defined, consistent and efficient hiring process—and then implement the specific, effective steps required to secure the best talent for your organization.
3. Identify the strategies, incentives and wrinkles needed to retain key talent in today’s candidate-driven market.
4. Position yourself to be in-demand talent.

Wednesday–Thursday April 15–16

Signature Series

Wednesday, April 15 • 8:45 – 9:45 AM
Talent Management: Best Practices for the Security Industry

The best companies know how to win and retain the best team members. Do you want top talent for your organization? Are you preparing yourself to be in-demand talent? Hiring and retaining people requires a significant amount of your time and dollars—and is crucial to your company’s bottom line. Learn how to develop both an efficient process and the desired culture to attract, hire and retain top talent in today’s candidate-driven market. Learn what you should be doing to prepare yourself to meet the evolving need for talent. Special attention will be paid to addressing the successful recruiting, hiring and retention trends for security manufacturers, integrators, alarm companies, distributors, consultants and end users. This interactive session will help you uncover what is working now and the importance of social media along the way.

Learning Objectives
1. Position yourself to be in-demand talent.
2. Identify the strategies, incentives and wrinkles needed to retain key talent in today’s candidate-driven market.
3. Increase your use of traditional, non-traditional and social media tools and practices to identify talent for your organization.

Thursday, April 16 • 8:45 – 9:45 AM
Making the Most of Big Data

We hear about it enough, but what is “big data” and how can it be used in a practical and actionable sense? How can we use it to gain actionable intelligence while it still matters? The Four-A Framework—Alert, Assess, Act and Analyze—empowers the promise of big data so that live, disconnected, often external, piles of data are molded into a timely, informed and actionable toolset with which emergency operations teams can act confidently and with clarity of vision.
Learning Objectives

1. Identify specific sources of information, including social media, that can inform your security operations.
2. Create an actionable strategy around maximizing the benefits of big data in your organization.
3. Determine methods that best utilize a person’s ability to think clearly and confidently in time-sensitive scenarios, and provide examples of this utility in the current state of the security industry.

Wednesday, April 15

Dealer, Installer, Integrator – Business Development

Wednesday, April 15 • 7:30 – 8:30 AM

Three Strategies to Combat Attrition and Why It Matters

While attrition is a key concept in the electronic security industry, it’s one of the most misunderstood. Your attrition rate directly affects the profitability of your alarm company and is a key value driver affecting what potential buyers are willing to pay for your accounts and/or business. In this session, participants learn how to calculate an accurate attrition rate, what the information really means to both your company and potential buyers, and why maintaining an attrition rate at or below industry standards is so important to both short- and long-term goals.

Learning Objectives

1. Define attrition and its causes.
2. Establish a formula to calculate your rate of attrition.
3. Identify the real difference between gross and net attrition, and why it matters to you and to your potential buyers.

Wednesday, April 15 • 10:00 – 11:00 AM

The Seven Deadly Sins of Alarm Contracts: Common Errors and How to Correct Them

There are seven common mistakes most often seen in security alarm contracts. Learn how to fix those mistakes and make your contracts more likely to be enforceable. Explore a recent law case that changed the way contracts are interpreted. Hear real-world examples of good and bad contracts, and how you can differentiate between the two. The session includes discussion of disclosures under the Federal Truth in Lending Act, must-haves for home solicitation sales, and best practices for alarm limitations of liability and subrogation waivers. Your take-away is an abundance of useful advice that you can implement on your own.

Learning Objectives

1. Correct your contracts so that they are more likely to be enforced.

Wednesday, April 15 • 11:15 AM – 12:15 PM

How to Survive in the Security Industry: The Next 10 Years

It’s one thing to think two to three years ahead, but what about ten years? Accompanied by tenured veterans of the security industry, visionaries in their own right, Dr. Bob Banerjee will facilitate a panel discussion that compares and contrasts the state of the industry ten years ago, now, and ten years in the future. What will we be selling? How will people buy and who will control the budget? Who will be the trusted advisors? Who are the new competitors likely to be? What role will the web play? The answers were different in 2004 compared to now, and are likely to be even more different in 2024. Attend this session for a look into the future and what it will take not only to survive, but to thrive.

Learning Objectives

1. Gain insight into the predicted long-term future of the security industry so you can identify the people you need to hire in order to succeed.
2. Specify the skills that will be required for success in the future.
3. Identify the kinds of partnerships you will need to form to maximize selling opportunities.

Wednesday, April 15 • 12:30 – 1:30 PM

How to Design, Package and Sell Service Agreements

It is a fact that most firms in the security industry do not sell service agreements, resulting in lower overall operating profits. This program is designed to help security system integrators and alarm dealers sell service agreements to their clients and prospects. Learn why firms buy service agreements, their needs, how to package the right program, how to sell them to both existing and new clients, and how to price them in accordance with growing market demand. All of the data in this presentation is based on the first-hand experience of the presenter who, in running two security firms, has used service agreements to propel his operating profits above 20%.

Learning Objectives

1. Design a service agreement to meet the immediate needs of your clients, including the different components and requirements.
2. Develop a proposal that will ensure 90% of your new clients purchase service agreements.
3. Price service agreements and time-and-materials labor to ensure a considerable increase in profitability.

Dealer, Installer, Integrator – Technology

Wednesday, April 15 • 7:30 – 8:30 AM

Evaluating New Technologies and Growth Opportunities in the Access Control, Video Surveillance and Smart Home Industries

The physical security market is ever-changing. New technology trends are impacting the traditional market structure and new equipment manufacturers are shifting the competitive landscape. This session helps you evaluate the key technologies that offer the best growth opportunity across the physical security market. A panelists of industry experts will examine the key technology trends in video surveillance, physical access control and the residential market. Providing market sizing and forecast data from published market reports to help you analyze the market opportunity, each panelist will outline the future outlook for his area of expertise. The discussion provides dealers, installers and integrators with a comprehensive overview of the physical security market, allowing them to make decisions that differentiate them from their competitors and develop a plan for success over the coming years.

Learning Objectives

1. Analyze the key technology trends in the video surveillance, access control and residential markets.
2. Evaluate how each technology trend fits with your business and identify opportunities and threats.
3. Develop a clear strategy to take advantage of new technology trends.
A multifaceted security industry carries one well-defined but often presumed thread of commonality—power provisioning. Rooted in societal activity awareness, this industry is typically equipment tethered to a “plug in the wall” operational resource. A myriad of hindrances impact our reliance on Big Grid electrical service, directly impacting security mission performance integrity. Assuming a backup outlet supply or providing off-grid operational resources have fundamental design concepts, components and ROI that will be identified in this session. Defining and presenting a proper customer power system solution entrenches an opportunity for daily user value but is sadly often ill-supported in the industry channel. Understanding the importance and basic technical details behind power systems drives customer identification, project suitability, and value delivery opportunity. Improper identification, assumptions, expectations, suitability and deployment complications create confusion, effort duplication and error impacting costs and utility. Join us as we expand the awareness of opportunity, balanced with fundamental knowledge, to ensure the operational integrity of security systems with properly designed power provisioning solutions.

Learning Objectives
1. Outline security system operational deployment and integrity issues impacted by power provisioning needs.
2. Identify project deployment power deficit considerations, the operational restrictions and potential impairment.
3. Design security system solutions implementing proper power provisioning considerations, ensuring operational deployment integrity.

Wednesday, April 15 • 12:30 – 1:30 PM
Adopting Mobile Credentials into Your Access Control Infrastructure
Join us to investigate the need for mobile access control credentials as our society evolves to demand increased convenience and security on a single device. This session addresses the evolution of the mobile credential to date, including perceptions by the security industry and by the general population of what is “secure enough” and what is needed in the future to meet that expectation. Examine the technologies that will enable this evolution today and tomorrow, including the pros and cons of NFC, HCE, BLE, Wi-Fi, iPhones and other coming opportunities and technologies that may enable our industry to move forward in satisfying the market need for secure and convenient credentials.

Learning Objectives
1. Identify the demand for increased security and convenience, including the need to improve the current state of credentials.
2. Describe why one credential type cannot fit the needs of all groups.
3. Identify the pros and cons of existing mobile credential technologies and their effect on credential issuing practices across different population groups.

Wednesday, April 15 • 11:15 AM – 12:15 PM
Welcome to Social Spaces: The Era of Social Access Management
The way people interact with buildings is changing. APs, mobile apps and wearable technology now make it possible to bridge virtual communities with physical spaces to enhance everyday experiences. Think how easy it is to get on a plane using your mobile device, especially if you are part of TSA PreCheck.

School Safety & Security
Wednesday, April 15 • 7:30 – 8:30 AM
Campus Police Investigations: How to Use CCTV to Solve Crimes and Increase Your Effectiveness
Gain insight into the various investigative tools CCTV can provide in a campus environment. Real-world examples will be used to show how you can reduce the hours needed to solve major crimes through proper placement of cameras, proper training of your security/dispatch and good detective work. Using actual footage from George Mason University’s Police Department, security experts show how CCTV footage can be used to successfully advance an investigation, present it in court and gain a conviction.

Learning Objectives
1. Define and describe the emerging market of Social Access Management.
2. Describe how social applications may be used in physical spaces to provide frictionless access control.
3. Identify use cases for where and how Social Access Management may be used to enhance everyday experiences.

Wednesday, April 15 • 10:00 – 11:00 AM
Active Shooter and Workplace Violence: It Can’t Happen Here!
Between 1992 and 2010, 13,827 people have been victims of active shooter or workplace violence in the United States. No state, industry or profession is immune. Yet people do not think it will ever happen where they work or live. Some businesses still do not have an active shooter or workplace violence plan or a process to report suspicious activity or potential issues. Even if a company has a plan, it is sometimes not communicated to all employees. This session outlines the five key elements in an active shooter and workplace violence plan, and focuses on the actions by and for businesses and employees. Don’t play the Las Vegas odds and think it will never happen to your organization. Instead take steps now to protect yourself, your customers and your business.

Learning Objectives
1. Identify the demand for increased security and convenience, including the need to improve the current state of credentials.
2. Decrease the hours needed to solve major crimes through proper placement of cameras, proper training of your security/dispatch and good detective work.
3. Identify the basic requirements for an effective CCTV operation to help drive savings in time and manpower.

Wednesday, April 15 • 10:00 – 11:00 AM
Active Shooter and Workplace Violence: It Can’t Happen Here!
Between 1992 and 2010, 13,827 people have been victims of active shooter or workplace violence in the United States. No state, industry or profession is immune. Yet people do not think it will ever happen where they work or live. Some businesses still do not have an active shooter or workplace violence plan or a process to report suspicious activity or potential issues. Even if a company has a plan, it is sometimes not communicated to all employees. This session outlines the five key elements in an active shooter and workplace violence plan, and focuses on the actions by and for businesses and employees. Don’t play the Las Vegas odds and think it will never happen to your organization. Instead take steps now to protect yourself, your customers and your business.

Learning Objectives
1. Identify the demand for increased security and convenience, including the need to improve the current state of credentials.
2. Decrease the hours needed to solve major crimes through proper placement of cameras, proper training of your security/dispatch and good detective work.
3. Identify the basic requirements for an effective CCTV operation to help drive savings in time and manpower.

Wednesday, April 15 • 11:15 AM – 12:15 PM
Case Study: How a University Used Facial Recognition Technology to Increase Residence Hall Safety
Controlling access to college residence halls is a major challenge primarily because students tend to move around campus in groups. When one student uses an ID card to open a residence door, several others might follow without presenting their own cards. This creates a security problem, as an accurate occupancy record is important for incident investigation and for making certain that everyone evacuates during an emergency. This case study explores how the University of San Francisco put its existing video surveillance technology to work in a new way—facial recognition. Because student moves in groups, the solution would need to recognize multiple faces, even those not facing the camera directly. Join us to learn the details of the USF system and the benefits of its use by other institutions and businesses.

Learning Objectives
1. Identify ways corporations and institutions can increase safety and security with video surveillance and facial recognition technology.
2. Explain how facial recognition technology reduces the costs of access security.
3. Determine how facial recognition eases access.

Wednesday, April 15 • 12:30 – 2:00 PM
The Israeli Approach to K-12 Security and Prevention
Led by a dedicated group of international security experts, civic leaders, educators and parents, the organization SERA has successfully pioneered groundbreaking measures that reduce and ultimately eliminate violence in education institutions at every level—from grade school to college and post-collegiate levels. SERA’s marriage of innovation, technology, experience, psychology and leadership has quantifiable results proving far more effective than any prior method ever implemented on U.S. soil. Drawing from case studies from around the world, SERA has replaced redundant and useless methods and spending with success methods undisclosed but employed by government agencies and private organizations worldwide to ensure absolute security in their specific applications. Learn how the extensive security background this panel of experts
Wednesday, April 15 • 12:30 – 1:30 PM
Security Operation Centers: Build Your Own, Virtualize or Both?

Should you build your own security operations center or virtualize it? Security executives looking to build a security operations center (SOC) face many challenges, among them a long planning process, pricey capital expenditures, design and construction costs, and post-build labor and operations. With the advances in technology, including cloud SaaS, off-premise hosting, hybrid cloud environments, and commercial off-the-shelf technology, there are more options for security directors to consider before either building out their own SOC or virtualizing it. In this session, seasoned security experts draw from real-world examples and success stories to help you assess your options and consider the benefits and challenges of building an internal SOC, virtualizing your operations to a third party or a combination of the two.

Learning Objectives
1. Approach SOC planning in a strategic, methodical way to avoid making the wrong decision.
2. Identify the technology options available for SOC planning.
3. Learn how to speak to senior executives as a business professional and not just the “security guy/gal.”

End User – IT Related

Wednesday, April 15 • 1:00 – 1:10 AM
The Evolving Cybersecurity Perimeter

In the last 10 years, securing valuable information has meant ‘securing the perimeter,’ such as firewalls and anti-virus engines, in an attempt to make the systems impenetrable to malicious outside parties. However, recent studies show that the greater threat comes from inside, particularly through valid users erroneously or maliciously allowing data to leak outside the organization. How can you lock down your data and systems so that even if a ‘trusted insider’ takes sensitive information outside the secure network perimeter it will be secure? New research targets data-centric information security techniques that ensure that sensitive data is identified, classified, marked and encrypted such that only those with valid credentials can use sensitive information, regardless of its location. To ensure the credentials are truly valid, this new data-centric approach is supported by ‘e-biometrics,’ a new technology that constantly analyzes a user’s pattern of interaction with the system, validating that the user entering the ID/password is, in fact, the person to whom the credentials were assigned. Join us to explore these exciting new best practices.

Learning Objectives
1. Understand how lifecycle management programs can be used for IP physical security systems.
2. Prepare and plan for the systems remediation process.
3. Establish a long-term financial model to support continuous improvement for physical security integrations.
Wednesday, April 15 • 11:15 AM – 12:15 PM
Hackers in Physical Security: Real-World Methods and Remediation

As businesses increasingly build shareholder value by investing and developing intellectual property, the risk of the intellectual property falling into the wrong hands also grows. Threats and attack methods are evolving and outpacing most physical security programs. It is often assumed that threats can be seen on cameras or that attacks only happen to IT systems. The truth is that physical security infrastructure is typically years behind IT; policies and practices are not updated against asset and risk assessments and hackers are generally lazy—they take the easy way in. As hackers become more familiar with physical security applications, controls and weaknesses, they are targeting organizations and going undetected to gain access to other areas to execute additional investigation and attacks to steal assets. This session takes attendees inside the mind of a real hacker—what they look for, how they do it, what they often find that organizations should fix immediately. This session highlights real-world examples, experiences and outcomes to help you analyze your environment and make substantial improvements that go beyond audit, compliance and certification.

Learning Objectives
1. Perform more effective risk based analysis against your assets.
2. Remediate the flaws in your current environment.
3. Analyze and validate steps with prospective vendors and integrators to ensure that applications are as secure as expected.

Wednesday, April 15 • 12:30 – 1:30 PM
End User – Public Safety

Smartphone Technology and Collaboration

End User – Public Safety

Wednesday, April 15 • 7:30 – 8:30 AM
Case Study: Redefining Law Enforcement Identification and Detection Capabilities Through Smartphone Technology and Collaboration

Among the many challenges facing law enforcement is obtaining accurate and rapid identification of a suspect or person of interest in the field. Often, officers still rely on the more primitive and often inaccurate information obtained through a field interview. However, the longer the officer has to wait to obtain information, the more he or she is put at risk. Learn how San Diego’s Association of Governments has pooled its resources and invested in technology to create a modern and more accurate real-time solution. By using smartphone applications and facial recognition technology designed specifically for law enforcement, officers in the field are more rapidly and accurately identifying suspects and zeroing in on the geo-location of suspicious activity. Learn how the investment has worked for San Diego and how its example could serve as a solution for you.

Learning Objectives
1. Source information necessary for establishing procurement requirements of a chemical detection system.
2. Determine integration requirements needed to provide a complete system.
3. Coordinate the development of internal and external Concepts of Operation (ConOps) and Standard Operating Procedures (SOPs) and understand system limitations for better response.

Wednesday, April 15 • 10:00 – 11:00 AM
Case Study: Integrating Chemical Detection, CCTV and Access Control for Enhanced Public Safety

How do you successfully implement a chemical detection system in an urban subway system while leveraging existing security systems and involving outside stakeholders? Installing a chemical detection system involves more than just procurement and installation of the chemical detection hardware and software. A system must reliably detect chemical threats with few false alarms. Additional information must be provided to first responders to gauge the threat level before endangering responding personnel. Other security systems may need to engage to prevent exposure to the community at large. Outside stakeholders must be actively involved in the process allowing them to modify or enhance their existing procedures. This session discusses the procurement, installation, integration and coordination methods used to implement a chemical detection system at a single Maryland Transit Administration Metro Station.

Learning Objectives
1. Outline the legal, technical and operational issues in cloud deployment.

Wednesday, April 15 • 11:15 AM – 12:15 PM
Cloud-Based Solutions for Law Enforcement: Navigating the Legal, Technical and Security Issues

With the proliferation of sensors and applications, the issue of data collection and storage is becoming increasingly important to security professionals. The cloud offers a potential solution, but the risks and rewards of cloud based solutions must be properly understood. This session examines the legal, technical and security considerations for cloud solutions. Discussion focuses on the critical issues law security professionals expect to confront as they evaluate and attempt to employ cloud-based solutions. The presentation highlights critical considerations and offers best practice for professionals to consider when developing and implementing cloud solutions for their data.

Learning Objectives
1. Analyze incidents and determine the proper level of risk to protect critical infrastructure facilities.
2. Select appropriate technology for the level of protection required to address the risk and vulnerabilities.
3. Address management challenges to security improvements and costs, and address how to present your case.

Wednesday, April 15 • 12:30 – 1:30 PM
Case Study: Physical Security Innovation for Critical Infrastructure Electrical Power and Transmission Facilities

Protection of critical infrastructure has gained visibility and momentum from the highly publicized gunfire attacks on power transmission facilities around the country. This session serves to familiarize security professionals with one particular incident, the investigation that followed, the risk and vulnerability analysis, resultant design criteria for risk abatement and protection, and the numerous project and culture challenges. Also learn about the physical security vulnerabilities and concerns of other critical infrastructure industries, such as pipelines, dams and chemical facilities. A focus will be applied on determining the appropriate level of protection, appropriate application of technology and team member dynamics.

Learning Objectives
1. Examine the advantages of smartphones and tablets for police officers in the field.
2. Explore potential solutions and the measures needed to implement mobile applications.
3. Illustrate how mobile reporting provides for geo-location reporting of suspicious activity correlated to critical infrastructure or protective areas of concern.
4. Evaluate the steps needed for a successful collaboration.

Wednesday, April 15 • 11:15 AM – 12:15 PM

Learning Objectives
1. Proactively address CIOs key concerns and questions.
2. Prepare the key questions and concerns you have for your CIO.
3. Identify and manage the common pitfalls in the relationship between physical security and IT staff.

Learning Objectives
1. Analyze and validate steps with prospective vendors and integrators to ensure that applications are as secure as expected.
2. Remediate the flaws in your current environment.
3. Illustrate how mobile reporting provides for geo-location of suspicious activity correlated to critical infrastructure or protective areas of concern.

Learning Objectives
1. Source information necessary for establishing procurement requirements of a chemical detection system.
2. Determine integration requirements needed to provide a complete system.
3. Coordinate the development of internal and external Concepts of Operation (ConOps) and Standard Operating Procedures (SOPs) and understand system limitations for better response.

Learning Objectives
1. Analyze the advantages of smartphones and tablets for police officers in the field.
2. Explore potential solutions and the measures needed to implement mobile applications.
3. Illustrate how mobile reporting provides for geo-location reporting of suspicious activity correlated to critical infrastructure or protective areas of concern.
4. Evaluate the steps needed for a successful collaboration.
and the bearer. There has been much discussion as to how well current primary IDs can be authenticated given their number, variety and lack of deliberately added security features. This session focuses on the various methods used to improve security documents and related procedures that help combat the growing acts of fraud, terrorism, illegal immigration, identity theft and other criminal acts.

**Learning Objectives**
1. Outline the difficulties in screening persons for possible imposter fraud or security and the inability of even a trained person to recognize valid documents.
2. Discuss the Breeder Document Standardized security features.
3. Identify the key elements of Identity, Credentialing and Access Management.

---

**Thursday, April 16 • 10:00 – 11:00 AM**

**Getting the Most Out of Biometric Technology**

Biometric technology can provide tremendous value when integrated into existing workflows. Properly implemented biometric technology can simplify tasks, reduce expenses, improve business productivity, enhance the end-user experience and increase security. Understanding your key drivers and stakeholders are essential to achieving successful ROI. Find out how to avoid the challenges of implementation—real or perceived—to deliver better business outcomes. This session provides valuable insight into criteria for the successful selection, design and implementation of biometric solutions. Gain lessons learned from the perspectives of the integrator, end user and biometric specialist. Several projects in which biometric technology was integrated into existing workflows are examined. Discover the true value proposition of biometric integration and what needs to be done to guarantee successful results.

**Learning Objectives**
1. Evaluate workflows that would benefit from biometric technology integration.
2. Differentiate real and perceived challenges to biometric technology integration.
3. Apply best practices and demonstrate ROI.

---

**Thursday, April 16 • 11:15 AM – 12:15 PM**

**Enabling Compliance for Physical and Cyber Security in Mobile Devices**

As mobile devices proliferate in your organization and as your users migrate more and more of their activities onto smartphones and tablets, how do you manage compliance in the cyber and physical world? Users are reading email on their phones, accessing secure websites using tablets and, in advanced scenarios, using credentials in their phones to unlock doors and log on to computers. To comply with internally- and externally-mandated policies, it is essential to manage the identities and associated credentials used. Join us to learn about the mobile ecosystem and how the different components work together to secure access. Primary use cases illustrate the need for and mechanisms to deliver compliance. The concept of an “Identity Perimeter” is introduced and its importance for compliance explained.

**Learning Objectives**
1. Discuss the options and security levels available for storing and managing identity in mobile devices.
2. Identify three options for establishing an identity perimeter in a mobile device.
3. Evaluate three different models for managing identity in mobile devices.

---

**Thursday, April 16 • 11:15 AM – 12:15 PM**

**You Own the Door, So Don’t Leave Dollars at the Threshold!**

Anytime you add a door position switch or multiple access control components to an opening, you become the owner of that door opening. Since you own the door, you shouldn’t be leaving money at the threshold for others! Owners are ready and willing to purchase new innovative solutions and aesthetically appealing products. Are you ready to provide these options? Wish more and more security technology being deployed “on-the-door” as opposed to “around-the-door” it’s imperative that managers and owners of security systems integration businesses understand the value in making this technology an integral part of their bid and service work. This session reviews the basic door components, identifies what gets modified by systems integrators and their sub-contractors, identifies the codes and standards that apply to electrified openings, outlines how green codes and sustainability will affect your future business, and explores the current and future state of integrated technology. Participants receive a workbook with reference links.

**Learning Objectives**
1. Identify the basic door components.
2. Identify the codes and standards applied to electrified openings.
3. Access the current and future state of integrated technology related to doors.

---

**Thursday, April 16 • 7:30 – 8:30 AM**

**Video Surveillance Trends: Adapt or Risk Obsolescence**

In a crowded market, security integrators, resellers, VARs and company security directors must wade through a myriad of industry news and data to stay at the top of their game. This roundtable discussion features an unbiased group of leading security editors and analysts who are the watchdogs of critical trends. Join us as they present the findings of a major independent industry survey of 500 respondents and share their views on the top trends and opportunities for 2015. The topics span video surveillance systems technology, camera technologies, cloud video surveillance, and/or applications for security or business operations. Ask your questions and share your real-world experiences, too.

**Learning Objectives**
1. Identify top industry trends that may affect your business.
2. Gain multiple perspectives on the various trends and topics to better inform your viewpoint.
3. Track future news and announcements with a more knowledgeable framework.
Thursday, April 16 • 10:00 – 11:00 AM
Connecting Your Video System to the Internet: Mitigating Your Security Vulnerabilities and Threats

With a focus on modern cyber security issues facing the physical security industry, discover a new approach to address concerns surrounding cloud-based video surveillance and IT security. Cyber security failings like the recent Heartbleed vulnerability have brought the issue of Internet security to the forefront of the world’s attention. It is important to gain insight on how to identify the vulnerabilities of a system and identify your adversaries. In this session, you learn how to better mitigate these threats and, in the process, build a system that is secure and simple to deploy, effectively manages bandwidth utilization and, for integrators, provides a new stream of recurring revenue.

**Learning Objectives**

1. Apply tactics to protect yourself against cyber security threats in a comprehensive way.
2. Identify the vulnerabilities of your video surveillance system to cyber security threats.
3. Assess the full extent of damage a cyber security threat poses to a business.

---

**Thursday, April 16 • 11:15 AM – 12:15 PM**

Beyond the Buzz: A Balanced Look into the Future of Physical Security

In years past, choosing technology meant that it would function for the next decade or two until replaced. Proprietary systems that operated in silos were acceptable since there were few requirements for interoperability. However, countering new threats models and delivering value to the business beyond being an operational cost center are driving new requirements and introducing new technology along with it. This session examines recent research and surveys that will guide a panel of top industry innovators, implementers and practitioners through a balanced, thoughtful and in-depth discussion into how various categories of physical security will change over the next decade. Join us to learn how to more effectively analyze your current program’s alignment with the next wave of threats and technology and design road maps that consider key principles to phase technology into your organization. Learn how to apply vendor-agnostic implementation strategies, while reducing capital investment typically required to embrace next generation technology.

**Learning Objectives**

1. Effectively analyze your current program’s alignment with the next wave of threats and technology.
2. Design program roadmaps that consider key principles to phase technology into your organization.
3. Apply vendor-agnostic implementation strategies while reducing capital investment typically required to embrace next generation technology.

---

**Thursday, April 16 • 12:30 – 1:30 PM**

Security Operations Centers: Providing the “Last Mile”

Today’s Security Operations Centers (SOC) are providing the basics—alarm and event management, written policies and procedures, operator training programs and cross-group coordination (facilities, ERT and local first responders). The reality is that they are only using a small percentage of the technology they already have in-house. In this session, you learn how to effectively integrate those technologies to reduce the noise by using video pop-ups, alarm prioritization, automated action plans, etc., so you can focus on real security issues that will free up the SOC to add additional value to the corporation (central point for facilities request, intelligent travel, corporate events, production monitoring, etc.)

**Learning Objectives**

1. Better utilize your existing technology.
2. Add value to your corporation above security items.
3. Become a customer-centric SOC.

---

**Thursday, April 16 • 10:00 – 11:00 AM**

The Fast Lane for Healthcare Security Leadership Success

Designed for novice through senior level healthcare security leaders, this session explores 11 key dynamics centered on ensuring the successful delivery of security in patient care-focused healthcare environments. Learn proven healthcare security leadership fundamentals and keys to success. Explore successful philosophies and the manner to integrate strong security practices and leadership into healthcare culture, mission and individual system branding. Superb solid and critical thinking skills, integrated into proven key elements, enrich the success of the security department and leadership.

**Learning Objectives**

1. Identify and maximize key success factors for healthcare security leaders.
2. Implement proven strategies.
3. Identify critical information, process and recommendations for success as a healthcare security leader.

---

**Thursday, April 16 • 11:15 AM – 12:15 PM**

Case Study: Lessons from the $1B San Diego International Airport Design-Build Program

Join us to learn about the key details and lessons learned from the design, engineering, integration, installation, testing and commissioning of San Diego International Airport’s expanded security, network and building management systems as part of the $1B T2-West Terminal Expansion/“Green Build” Initiative. This master Design/Build initiative incorporated “fast-trac” construction processes and methods to ensure timely completion. The new terminal facilities provide state-of-art airline systems and applications for check-in, ticket processing, checked baggage inspection, passenger and property screening, and gate and ramp operations.

**Learning Objectives**

1. Better utilize your existing technology.
2. Add value to your corporation above security items.
3. Become a customer-centric SOC.

---

**Thursday, April 16 • 7:30 – 8:30 AM**

The Internet of Things: The Promise for the Security Industry

By connecting physical objects and sensors to networks, the Internet of Things allows devices to communicate with one another and deliver meaningful information. This improves safety and security, increases efficiency, enhances quality of life and ultimately changes how decisions are made. From home automation to global enterprise security management, the opportunities for bringing together people, data and things in new ways are endless. In this session, attendees gain an introduction to the Internet of Things, learn about current applications of this significant technological trend and explore the promise of the Internet of Things for the security industry. This must-attend session is designed for anyone interested in understanding the Internet of Things and its impact on the security industry.

**Learning Objectives**

1. Define the Internet of Things.
2. Identify ways in which the technology is currently being used.
3. Understand the promise of the Internet of Things for the security industry.

---

**Thursday, April 16 • 10:00 – 11:00 AM**

The Internet of Things: The Promise for the Security Industry

By connecting physical objects and sensors to networks, the Internet of Things allows devices to communicate with one another and deliver meaningful information. This improves safety and security, increases efficiency, enhances quality of life and ultimately changes how decisions are made. From home automation to global enterprise security management, the opportunities for bringing together people, data and things in new ways are endless. In this session, attendees gain an introduction to the Internet of Things, learn about current applications of this significant technological trend and explore the promise of the Internet of Things for the security industry. This must-attend session is designed for anyone interested in understanding the Internet of Things and its impact on the security industry.

**Learning Objectives**

1. Define the Internet of Things.
2. Identify ways in which the technology is currently being used.
3. Understand the promise of the Internet of Things for the security industry.
Thursday, April 16 • 10:00 – 11:00 AM
Protecting Your Intellectual Property and Corporate Data While Traveling

Learn how a corporation’s critical intellectual property and proprietary processes can be compromised and stolen while its employees travel on company business. This session provides an overview of common schemes used by hostile governments or competitors in exfiltrating data containing IP or other proprietary material. Learn of the vulnerability of iPhones, iPads and other phones and tablets to data compromise and of the risks employees face when they encounter a competitor or a hostile government official who is skilled in social engineering techniques or spear “phishing.”

Learning Objectives
1. Identify what constitutes intellectual property within your firm or corporation.
2. Identify the specific risks and vulnerabilities to your company data and that reach critical levels when company officials travel with corporate data, processes or secrets.
3. Initiate specific measures to mitigate the risk to intellectual data and corporate processes while traveling, while retaining access to information required for a productive trip.

Thursday, April 16 • 11:15 AM – 12:15 PM
Criminal Pattern Identification and the Philosophy of Big Data

How does a city analyze crime statistics and then execute crime prevention? Can crime mapping reveal problem locations not considered previously? Temporal crime analysis can often reveal trends for different times and locations in a city. Today’s crime fighting team now often includes persons experienced in crime analysis and psychology to explain and sometimes predict a higher possibility of data center breaches, business interruption and violent crime. Experience a fresh, multimedia take on the various philosophies relevant to Big Data and relevant to all the things you need to protect your operation. Consider the unique viewpoints of IT management, police, attorneys and physical security professionals in the review of crime data and predictions.

Learning Objectives
1. Discuss the role of Big Data in data review and crime prevention.
2. Leverage real-world success stories.
3. Explore how IT management, police, attorneys and physical security professionals can and should work together.

Thursday, April 16 • 12:30 – 1:30 PM
Mobile and Connected Commerce: A Game Changer or Security Nightmare?

Near field communication (NFC) technology has brought an opportunity for mobile and connected commerce that may only be realized through the use of host card emulation (HCE). In this session, a group of experts explore real-life NFC/HCE implementations across various verticals and assess the potential game-changing aspects of HCE and associated security concerns.

Learning Objectives
1. Define NFC and HCE.
2. Identify potential benefits and security risks related to NFC/HCE implementations.

Education Session Pricing Options

SIA Education@ISC West offers various pricing packages, so you can always stay within your budget.

<table>
<thead>
<tr>
<th>Package</th>
<th>EARLY BIRD (Valid through 2/23/2015)</th>
<th>REGULAR (Valid after 2/23/2015)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Three-Day Package</td>
<td>$825</td>
<td>$925</td>
</tr>
<tr>
<td>Two-Day Package</td>
<td>$625</td>
<td>$725</td>
</tr>
<tr>
<td>One-Day Package</td>
<td>$425</td>
<td>$525</td>
</tr>
<tr>
<td>Single Session Pass</td>
<td>$150</td>
<td></td>
</tr>
</tbody>
</table>

If you have questions on education pricing or need further assistance, please contact Katelyn Battinelli at 203-840-5876.

For more about SIA Education@ISC West, visit us at http://www.iscwest.com/Education/