SIA education @ISC
Sands Expo
Las Vegas, NV
APRIL 5-7, 2016

CONFERENCE PROGRAM

PLATINUM SPONSOR
AXIS COMMUNICATIONS
VIDEO SURVEILLANCE TRACK SPONSOR
Onvif® The IP-based Security Standard
### Sessions-at-a-Glance

#### Tuesday, April 5

<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>WORKSHOP: Dealing with Today’s Active Shooters (Workshop #1)</td>
<td>Workshops 201</td>
<td>204</td>
</tr>
<tr>
<td>8:00 – 10:00 AM</td>
<td>WORKSHOP: Developing the Problem-Solving Mindset (Workshop #2)</td>
<td>Workshops 207</td>
<td>207</td>
</tr>
<tr>
<td>8:30 – 10:00 AM</td>
<td>Taking the Edge Off of Systems Integration</td>
<td>PSA Track</td>
<td>209</td>
</tr>
<tr>
<td>8:30 – 10:00 AM</td>
<td>Are We Secure? Business Know-How for the Risk Discussion</td>
<td>End User - Strategic Management</td>
<td>304</td>
</tr>
<tr>
<td>8:30 – 9:30 PM</td>
<td>IAPSC Successful Security Consulting Seminar</td>
<td>IAPSC</td>
<td>302</td>
</tr>
<tr>
<td>8:30 – 11:15 AM</td>
<td>Video Analytics: The Real Past and the Imagined Future</td>
<td>PSA Track</td>
<td>209</td>
</tr>
<tr>
<td>10:30 – 12:30 AM</td>
<td>ADDRESSING CYBER SECURITY WITH PROTECTIVE MEASURES TO ENSURE THE FUTURE</td>
<td>Workshops 307</td>
<td>307</td>
</tr>
<tr>
<td>10:30 – 12:30 AM</td>
<td>The Hottest IT Skills in the Physical Security Space</td>
<td>PSA Track</td>
<td>209</td>
</tr>
<tr>
<td>11:30 AM – 12:30 PM</td>
<td>Addressing Cyber Work by Protecting Your Facilities and Infrastructure Beyond the Physical Realm</td>
<td>End User - Strategic Management</td>
<td>304</td>
</tr>
<tr>
<td>12:30 – 1:30 PM</td>
<td>Lunch in the Conference Attendee Lounge (Three-day package only)</td>
<td>PSA Track</td>
<td>209</td>
</tr>
<tr>
<td>1:30 – 2:30 PM</td>
<td>Cyber Security - How to Ensure Your Vendors Are Not Leaving You Vulnerable</td>
<td>Special Programming</td>
<td>307</td>
</tr>
<tr>
<td>1:30 – 2:30 PM</td>
<td>The Internet of Things and Security Solutions: Transforming Security from a Cost Center to a Value Center</td>
<td>End User - Strategic Management</td>
<td>304</td>
</tr>
<tr>
<td>1:30 – 3:00 PM</td>
<td>WORKSHOP: Cyber Security and You: The Future of Physical Access in a Digital World (Workshop #1)</td>
<td>Workshops 307</td>
<td>307</td>
</tr>
<tr>
<td>2:45 – 3:45 PM</td>
<td>Case Study: Rolling Out Business Intelligence with Superior ROI</td>
<td>End User - Strategic Management</td>
<td>304</td>
</tr>
<tr>
<td>3:30 – 5:00 PM</td>
<td>WORKSHOP: Cyber Security and You: The Future of Physical Access in a Digital World (Workshop #2)</td>
<td>Workshops 307</td>
<td>307</td>
</tr>
<tr>
<td>4:00 – 5:00 PM</td>
<td>How to Implement a Life Cycle Management Program</td>
<td>PSA Track</td>
<td>209</td>
</tr>
<tr>
<td>4:00 – 5:00 PM</td>
<td>State of the Security Industry and its Future</td>
<td>End User - Strategic Management</td>
<td>304</td>
</tr>
</tbody>
</table>

---

### Sessions-at-a-Glance

#### Wednesday, April 6

<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>Protection on the Edge Using Edge Technology and Remote Site Monitoring to Protect Your Most Valuable Assets</td>
<td>Special Programming</td>
<td>307</td>
</tr>
<tr>
<td>7:30 – 8:30 AM</td>
<td>Integrators Meeting the Challenge</td>
<td>Dealer, Installer, Integrator Technology</td>
<td>309</td>
</tr>
<tr>
<td>7:30 – 8:30 AM</td>
<td>CCTV 101: The Basics and Beyond</td>
<td>Video Surveillance</td>
<td>304</td>
</tr>
<tr>
<td>7:30 – 8:30 AM</td>
<td>Medical Marijuana Facilities: Maintaining Comprehensive Security in a Dynamic Industry</td>
<td>End User - Physical Security Issues</td>
<td>302</td>
</tr>
<tr>
<td>7:30 – 8:30 AM</td>
<td>Clarifying Event-Related Procedures for Digital Video and Admissibility</td>
<td>Special Programming</td>
<td>307</td>
</tr>
<tr>
<td>8:45 – 9:45 AM</td>
<td>Lights, Camera Action! How Paramount Pictures Delivers Enhanced Safety and Global Security While Driving Operational Efficiency and Sustainable ROI</td>
<td>Signature Series</td>
<td>304</td>
</tr>
<tr>
<td>10:00 – 11:00 AM</td>
<td>Keeping the Backend Up: Operational, Policy, and Technology Considerations for Managing Risk</td>
<td>Special Programming</td>
<td>307</td>
</tr>
<tr>
<td>10:00 – 11:00 AM</td>
<td>Disruptive Technology, Innovation and You</td>
<td>Dealer, Installer, Integrator Technology</td>
<td>309</td>
</tr>
<tr>
<td>10:00 – 11:00 AM</td>
<td>Have We Over-Engineered the Video Surveillance Industry?</td>
<td>Video Surveillance</td>
<td>304</td>
</tr>
<tr>
<td>10:30 – 11:30 AM</td>
<td>Solving the Whole Picture: Enhanced Coverage and Business Intelligence with 360-Degree Technology</td>
<td>End User - Physical Security Issues</td>
<td>302</td>
</tr>
<tr>
<td>11:15 AM – 12:15 PM</td>
<td>Counteracting the Threat of Drones</td>
<td>Special Programming</td>
<td>307</td>
</tr>
<tr>
<td>11:15 AM – 12:15 PM</td>
<td>Taking a Full Cycle Approach to CCTV Deployment</td>
<td>Video Surveillance</td>
<td>304</td>
</tr>
<tr>
<td>11:15 AM – 12:15 PM</td>
<td>The Growing Need for Mass Notification and Emergency Communications</td>
<td>End User - Public Safety</td>
<td>304</td>
</tr>
<tr>
<td>12:30 – 1:30 PM</td>
<td>The Internet of Home Next Generation Security and Smart Home Control</td>
<td>Special Programming</td>
<td>307</td>
</tr>
<tr>
<td>12:30 – 1:30 PM</td>
<td>Solving the VMS Searchability Problem</td>
<td>Dealer, Installer, Integrator Technology</td>
<td>309</td>
</tr>
<tr>
<td>12:30 – 1:30 PM</td>
<td>Dark Nights: How to Overcome Key Challenges</td>
<td>Video Surveillance</td>
<td>304</td>
</tr>
<tr>
<td>12:30 – 1:30 PM</td>
<td>Preparing for Physical Security Requirements of CP-014: Designing a Sustainable Early Warning System</td>
<td>End User - Physical Security Issues</td>
<td>302</td>
</tr>
<tr>
<td>1:45 – 2:45 PM</td>
<td>Camera Apps Other in a New Era in Surveillance System Design</td>
<td>Video Surveillance</td>
<td>304</td>
</tr>
<tr>
<td>2:30 – 3:30 PM</td>
<td>Exhibit Hall Opening</td>
<td>Special Programming</td>
<td>307</td>
</tr>
</tbody>
</table>
## Sessions-at-a-Glance

### Thursday, April 7

<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>Impact of Enterprise Security Risk Assessments on Integrators &amp; Manufacturers</td>
<td>Dealer, Installer, Integrator</td>
<td>302</td>
</tr>
<tr>
<td>7:30 – 8:30 AM</td>
<td>Perimeter Intruder Detection for Electrical Power Generation, Transmission and Distribution Facilities</td>
<td>Video Surveillance</td>
<td>309</td>
</tr>
<tr>
<td>7:30 – 8:30 AM</td>
<td>Regulation through Litigation – Lessons from Recent Data Breach Lawsuits and Enforcement Actions</td>
<td>Security Sales Workshops</td>
<td>304</td>
</tr>
<tr>
<td>7:30 – 9:00 AM</td>
<td>SALES WORKSHOP: Creating Fully Engaged Customers</td>
<td>Access &amp; ID Management</td>
<td>307</td>
</tr>
<tr>
<td>7:30 AM – 4:30 PM</td>
<td>WORKSHOP: Critical Thinking for the Security Professional(All Day Session)</td>
<td>Workshops</td>
<td>305</td>
</tr>
<tr>
<td>8:45 – 9:45 AM</td>
<td>If You Only Knew What Hackers Can Do</td>
<td>Signature Series</td>
<td>201</td>
</tr>
<tr>
<td>10:00 – 11:00 AM</td>
<td>Access Control Trends in the Education Sector</td>
<td>Access &amp; ID Management</td>
<td>307</td>
</tr>
<tr>
<td>10:00 – 11:00 AM</td>
<td>New Technologies for IP Surveillance Video Retention</td>
<td>Video Surveillance</td>
<td>309</td>
</tr>
<tr>
<td>10:00 – 11:00 AM</td>
<td>The Seven Deadly Sins of Alarm Contracts: Common Errors and How to Correct Them</td>
<td>Dealer, Installer, Integrator</td>
<td>307</td>
</tr>
<tr>
<td>11:00 – 12:00 AM</td>
<td>The State of the Cloud in the Security Industry</td>
<td>Security Sales Workshops</td>
<td>304</td>
</tr>
<tr>
<td>10:00 – 11:30 AM</td>
<td>SALES WORKSHOP: New Age Selling - Technology-based Strategies to Drive Sales</td>
<td>Security Sales Workshops</td>
<td>304</td>
</tr>
<tr>
<td>11:15 AM – 12:15 PM</td>
<td>The Significant Technology Affecting IoT, Sensors and Analytics</td>
<td>Security Sales Workshops</td>
<td>304</td>
</tr>
<tr>
<td>11:30 AM – 12:30 PM</td>
<td>How to Design, Sell and Implement Service Agreements</td>
<td>Dealer, Installer, Integrator</td>
<td>307</td>
</tr>
<tr>
<td>12:00 – 1:30 PM</td>
<td>SALES WORKSHOP: Creating Fully Engaged Customers</td>
<td>Security Sales Workshops</td>
<td>304</td>
</tr>
<tr>
<td>12:30 – 1:30 PM</td>
<td>Touchless Biometric Secure Access Control for High Volume Versus from Academia To Zio</td>
<td>Access &amp; ID Management</td>
<td>307</td>
</tr>
<tr>
<td>12:30 – 1:30 PM</td>
<td>Survey Says: What IT &amp; University Campus Want For Video Surveillance</td>
<td>Video Surveillance</td>
<td>309</td>
</tr>
<tr>
<td>1:30 – 2:45 PM</td>
<td>The Latest in Open Space Video Surveillance Multi-sensor Camera Technology</td>
<td>Video Surveillance</td>
<td>309</td>
</tr>
<tr>
<td>2:45 – 3:00 PM</td>
<td>No Sessions—Exhibit Hall Open</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Tuesday, April 5

#### 8:00 – 10:00 AM

**WORKSHOP: Dealing with Today’s Active Shooters**

In today’s environment, active shootings have unfortunately maintained a very deadly and real threat for businesses and communities. Regardless of the business model or size, employees and guests have fallen victim to these vicious attacks that occur without warning or impunity. This hands-on workshop focuses on how a business and its employees are not silent observers in deadly emergencies, but a valuable partner who can provide clarity, assistance and guidance to the first responder community. While we are an information society that thrives on timely and actionable communications when facing barbaric acts, this session helps you discover the communications platform and infrastructure to determine the plan on who should dispatch these messages.

**Learning Objectives:**

1. Gain clarity on the business and employee response based on specific business offerings, while also considering the ‘duty of care’ responsibility which may hold the company liable for inaction, indecisiveness or inadequate training.

2. Determine how the method of “run, hide and fight” approach works under various business models and which liability exposures need to be addressed immediately in most organizations.

#### 8:30 – 10:00 AM

**Taking the Edge Off of Systems Integration**

Integrating multiple security systems in an effort to streamline management and reporting capabilities has great value to the end user, though it isn’t always as easy as it sounds. For instance, having multiple systems tools in place can create sensory overload issues for staff, for instance. Data should be easily accessible to be useful and interoperability must simplify versus complicate your process to make integration worthwhile. Collaborative vendor partnerships are critical to ensure integration engenders cooperation and efficiency. Join a discussion featuring consultants and systems integrators who have established their own winning formula for an end-to-end approach to systems integration.

**Learning Objectives:**

1. Discover how working with the right partners to help consolidate your systems can improve system efficiency without unnecessary complexity.

2. Simplify new services and technologies utilizing good program management, such as requirements planning, engineering and architecture, testing and by prioritizing developments for deployment.

3. Create new opportunities to become the trusted advisor by acting as the systems integration facilitator that bridges the gap between technical solutions to operational excellence and efficiency.

---

**SIA Education @ISC West Offers Various Registration Packages:**

http://www.iscwest.com/Education/Pricing/

**Special Thanks to our Generous Sponsor:**

Special Pricing!
8:30 – 10:00 AM Are We Secure? Business Know-How for the Risk Discussion

Communicating to the executive team can be a demanding task, but you don’t have to dread talking about your security posture. Stakeholders want to know which security initiatives are being instituted and ensure support is available for the project to be successful. But how do you explain that no matter how good your risk mitigation program is, no system can ever claim to be 100 percent secure? An interdisciplinary panel of risk management specialists will share how to address the risk potential of your organization and discuss the security program in terms business leaders can understand.

Learning Objectives:
1. Engage the executive team in a business conversation versus a purely security conversation regarding your risk mitigation program.
2. Identify key risk events that could derail the objectives of your strategic plan, including critical assets and associated impacts in business terms from financial, competitive, reputation, or regulatory perspectives.
3. Discuss the potential impact a security event can pose on various parts of the operations in everyday business terms.

8:30 AM – 5:00 PM Back by Popular Demand IAPSC Successful Security Consulting Seminar

The IAPSC Successful Security Consulting Seminar is offered as a set of sessions to be taken together to maximize the value of this seminar.

8:30 – 8:45 AM IAPSC SESSION 1: Successful Security Consulting: Introduction and Overview

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.

8:45 – 10:00 AM IAPSC SESSION 2: The Business of Security Consulting: From Consulting 101 to Becoming a Certified Security Consultant

In The Business of Security Consulting, participants learn the essential traits for success as a security consultant, how to build a practice, and how to add value to a client’s 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 each 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. These include the best ways to position your business and services, deal with competition and target a specific industry.

10:15 – 11:00 AM IAPSC SESSION 3: The Financial and Administrative Aspects of Security Consulting

Learn the essential administrative and accounting aspects of the consultant’s practice and how to administer the practice as a business on a day-to-day 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.

11:00 AM – 12:00 PM IAPSC SESSION 4: Proposing Security Consulting Services and Hiring a Security Consultant

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 versus competitive opportunities; how and when to prepare competitive written proposals; types of bid packages, proposals and the nature of the request for proposals (RFP, R.Q, R.B & Sources Sought); how to cost estimate a job, the various types of contractual relationships, and how to fully and completely respond to a bid.

1:00 – 2:00 PM IAPSC SESSION 5: Executing and Completing the Consulting Assignment

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 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 change 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 phased aspects 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.

2:00 – 3:00 PM IAPSC SESSION 6: Preparing a Responsive, High-Impact Consultant’s Report

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.


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 designer’s 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 definition the 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.


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 convergence 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.

4:45 – 5:00 PM IAPSC SESSION 9: Summary & Course Wrap-up
In today's environment, active shootings have unfortunately maintained a very deadly and real threat for businesses and communities. Regardless of the business model or size, employees and guests have fallen victim to these vicious attacks that occur without warning or impunity. This hands-on workshop focuses on how a business and its employees are not silent observers in deadly emergencies, but a valuable partner who can provide clarity, assistance and guidance to the first responder community. While we are an information society that thrives on timely and actionable communications when facing barbaric acts, this session helps you discover the communications platform and infrastructure to determine the plan on who should dispatch these messages.

Learning Objectives:
1. Establish which IT skills will net more value to the growth of your operation and services portfolio.
2. Discover which certifications will insure the kind of expertise that will help you to navigate today's technology trends affecting business.
3. Recommend industry sources that can help to catalog, analyze and classify your choices based on your present and future business needs.

11:30 AM - 12:30 PM
Addressing Cyber Risks by Protecting your Facilities and Infrastructure Beyond the Physical Realm

Daily waves of cyber threats to data and infrastructure present challenges and opportunities. Those willing to steal data or create general acts of espionage and terrorism continually look for ways to access sensitive data and commit fraud and impact systems and infrastructure. It's imperative those deploying security solutions consider all aspects of cyber risk mitigation. Threats are ever evolving and more agile as malcontents use new and sophisticated methods to exploit defenses. Security solution advancements need to be properly deployed in order to realize their benefits. You'll hear how to prioritize threats to physical security solutions, which guidance, security controls and standards to consider and the components for long term implementation.

Learning Objectives:
1. Identify overlapping, redundant functions and become sensitized to the broader corporate strategies impacting security in a cost cutting environment.
2. Advance the consolidation wave and assume a leadership role in integrating various overlapping functions.
3. Explain the importance of proactive risk management, transforming the security organization into the most reliable source of information within the enterprise.

11:30 AM - 12:30 PM
WORKSHOP: Dealing with Today's Active Shooters

This unique, highly interactive workshop coaches participants to think through problems in a systematic manner, a skill applicable to any position or industry. Through a series of real-life scenarios, each representing a different obstacle to problem solving that increases in complexity, workshop participants discover how to ask quality questions and identify pieces of information that are critical to success. Gain increased risk management skills and future business needs.

Learning Objectives:
1. Gain clarity on the business and employee response based on specific business offerings, while also considering the 'duty of care' responsibility which may hold the company liable for inaction, indifference or inadequate training.
2. Determine how the method of "run, hide and fight" approach works under various business models and how business expenses need to be addressed immediately in most organizations.

10:30 AM - 12:30 PM
WORKSHOP: Developing the Problem-Solving Mindset

In today's environment, active shootings have unfortunately maintained a very deadly and real threat for businesses and communities. Regardless of the business model or size, employees and guests have fallen victim to these vicious attacks that occur without warning or impunity. This hands-on workshop focuses on how a business and its employees are not silent observers in deadly emergencies, but a valuable partner who can provide clarity, assistance and guidance to the first responder community. While we are an information society that thrives on timely and actionable communications when facing barbaric acts, this session helps you discover the communications platform and infrastructure to determine the plan on who should dispatch these messages.

Learning Objectives:
1. Establish which IT skills will net more value to the growth of your operation and services portfolio.
2. Discover which certifications will insure the kind of expertise that will help you to navigate today's technology trends affecting business.
3. Recommend industry sources that can help to catalog, analyze and classify your choices based on your present and future business needs.

11:30 AM - 12:30 PM
Addressing Cyber Risks by Protecting your Facilities and Infrastructure Beyond the Physical Realm

Daily waves of cyber threats to data and infrastructure present challenges and opportunities. Those willing to steal data or create general acts of espionage and terrorism continually look for ways to access sensitive data and commit fraud and impact systems and infrastructure. It's imperative those deploying security solutions consider all aspects of cyber risk mitigation. Threats are ever evolving and more agile as malcontents use new and sophisticated methods to exploit defenses. Security solution advancements need to be properly deployed in order to realize their benefits. You'll hear how to prioritize threats to physical security solutions, which guidance, security controls and standards to consider and the components for long term implementation.

Learning Objectives:
1. Identify overlapping, redundant functions and become sensitized to the broader corporate strategies impacting security in a cost cutting environment.
2. Advance the consolidation wave and assume a leadership role in integrating various overlapping functions.
3. Explain the importance of proactive risk management, transforming the security organization into the most reliable source of information within the enterprise.

10:30 AM - 12:30 PM
WORKSHOP: Dealing with Today’s Active Shooters

In today’s environment, active shootings have unfortunately maintained a very deadly and real threat for businesses and communities. Regardless of the business model or size, employees and guests have fallen victim to these vicious attacks that occur without warning or impunity. This hands-on workshop focuses on how a business and its employees are not silent observers in deadly emergencies, but a valuable partner who can provide clarity, assistance and guidance to the first responder community. While we are an information society that thrives on timely and actionable communications when facing barbaric acts, this session helps you discover the communications platform and infrastructure to determine the plan on who should dispatch these messages.

Learning Objectives:
1. Establish which IT skills will net more value to the growth of your operation and services portfolio.
2. Discover which certifications will insure the kind of expertise that will help you to navigate today's technology trends affecting business.
3. Recommend industry sources that can help to catalog, analyze and classify your choices based on your present and future business needs.

10:30 AM - 12:30 PM
WORKSHOP: Developing the Problem-Solving Mindset

This unique, highly interactive workshop coaches participants to think through problems in a systematic manner, a skill applicable to any position or industry. Through a series of real-life scenarios, each representing a different obstacle to problem solving that increases in complexity, workshop participants discover how to ask quality questions and identify pieces of information that are critical to success. Gain increased risk management skills and future business needs.

Learning Objectives:
1. Establish which IT skills will net more value to the growth of your operation and services portfolio.
2. Discover which certifications will insure the kind of expertise that will help you to navigate today's technology trends affecting business.
3. Recommend industry sources that can help to catalog, analyze and classify your choices based on your present and future business needs.

11:30 AM - 12:30 PM
Addressing Cyber Risks by Protecting your Facilities and Infrastructure Beyond the Physical Realm

Daily waves of cyber threats to data and infrastructure present challenges and opportunities. Those willing to steal data or create general acts of espionage and terrorism continually look for ways to access sensitive data and commit fraud and impact systems and infrastructure. It's imperative those deploying security solutions consider all aspects of cyber risk mitigation. Threats are ever evolving and more agile as malcontents use new and sophisticated methods to exploit defenses. Security solution advancements need to be properly deployed in order to realize their benefits. You'll hear how to prioritize threats to physical security solutions, which guidance, security controls and standards to consider and the components for long term implementation.

Learning Objectives:
1. Identify overlapping, redundant functions and become sensitized to the broader corporate strategies impacting security in a cost cutting environment.
2. Advance the consolidation wave and assume a leadership role in integrating various overlapping functions.
3. Explain the importance of proactive risk management, transforming the security organization into the most reliable source of information within the enterprise.

10:30 AM - 12:30 PM
WORKSHOP: Dealing with Today’s Active Shooters

In today’s environment, active shootings have unfortunately maintained a very deadly and real threat for businesses and communities. Regardless of the business model or size, employees and guests have fallen victim to these vicious attacks that occur without warning or impunity. This hands-on workshop focuses on how a business and its employees are not silent observers in deadly emergencies, but a valuable partner who can provide clarity, assistance and guidance to the first responder community. While we are an information society that thrives on timely and actionable communications when facing barbaric acts, this session helps you discover the communications platform and infrastructure to determine the plan on who should dispatch these messages.

Learning Objectives:
1. Establish which IT skills will net more value to the growth of your operation and services portfolio.
2. Discover which certifications will insure the kind of expertise that will help you to navigate today's technology trends affecting business.
3. Recommend industry sources that can help to catalog, analyze and classify your choices based on your present and future business needs.

10:30 AM - 12:30 PM
WORKSHOP: Developing the Problem-Solving Mindset

This unique, highly interactive workshop coaches participants to think through problems in a systematic manner, a skill applicable to any position or industry. Through a series of real-life scenarios, each representing a different obstacle to problem solving that increases in complexity, workshop participants discover how to ask quality questions and identify pieces of information that are critical to success. Gain increased risk management skills and future business needs.

Learning Objectives:
1. Establish which IT skills will net more value to the growth of your operation and services portfolio.
2. Discover which certifications will insure the kind of expertise that will help you to navigate today's technology trends affecting business.
3. Recommend industry sources that can help to catalog, analyze and classify your choices based on your present and future business needs.

11:30 AM - 12:30 PM
Addressing Cyber Risks by Protecting your Facilities and Infrastructure Beyond the Physical Realm

Daily waves of cyber threats to data and infrastructure present challenges and opportunities. Those willing to steal data or create general acts of espionage and terrorism continually look for ways to access sensitive data and commit fraud and impact systems and infrastructure. It's imperative those deploying security solutions consider all aspects of cyber risk mitigation. Threats are ever evolving and more agile as malcontents use new and sophisticated methods to exploit defenses. Security solution advancements need to be properly deployed in order to realize their benefits. You'll hear how to prioritize threats to physical security solutions, which guidance, security controls and standards to consider and the components for long term implementation.

Learning Objectives:
1. Prioritize threats to your infrastructure and create a plan to determine risk for better security controls.
2. Apply security control sets that introduce technical assessment concepts and related tools for cyber security.
3. Set goals and requirements when selecting a response plan and implementation beyond the component or sub-system level.

1:30 – 2:30 PM
Cyber Security - How to Ensure Vendors Are Not Leaving You Vulnerable

You're preparing for an upcoming project or service contract and finalizing the RFP. There are important questions you should ask when it comes to cyber security and enterprise resilience tactics. Join experts to determine how to evaluate, qualify and disqualify potential partners based on their cyber security and disaster recovery policies. Discuss key characteristics of a responsible information and network security program and best practices in managing ongoing vendor relationships and red flags in the prequalification process.

Learning Objectives:
1. Create a vendor questionnaire template for RFPs.
2. Determine a list of top 10 Musts and Must Nots, and a list of resources for future reference and further education.

1:30 – 2:30 PM
The Internet of Things and Security Solutions: Transforming Security from a Cost Center to a Value Center

IoT describes the proliferation of connected sensors and devices, a phenomenon that has not only changed our technology landscape, but is also directly influencing the realm of security. Traditionally, security solutions have been put in place to target the challenges of theft and damage to property, but with the proliferation of IoT, how can security professionals show return on investment outside of physical security? Gain insights about the role IoT plays in security and the three ways today’s security solutions can transform video from raw data into actionable insights, generate measurable impact on business strategy and improve an organization’s bottom line.

Learning Objectives:
1. Examine the Internet of Things as it applies to the security space.
2. Evaluate new business intelligence solutions techniques.
3. Apply business intelligence strategies to current security projects to improve system design and increase ROI for the end user.
1:30 – 3:30 PM and 3:30 – 5:00 PM

WORKSHOP: Cyber Security and You: The Future of Physical Access in a Digital World

Today’s mobile world has the potential to profoundly change our industry and how we look at physical access controls. The prospect of a more seamless and secure user experience while eliminating expensive infrastructure is just around the corner. If implemented poorly, however, these deployments could introduce significant risk to organizations. As we do more with our mobile phones and increasingly demand anywhere/anytime access, the opportunity to better protect these activities while creating a more satisfying, mobile-centric security experience at home, in the office and on the road brings the “future” into the present.

Learning Objectives:
1. Explore the increasingly interconnected and mobile world is impacting physical security.
2. Identify and recognize how digital systems and access controls are impacting physical security and the user experience.
3. Review lessons learned from the digital world that are shaping physical access in security across many industry verticals.
4. Ascertain the process to prepare for this mobile device deployment transition and mitigate organizational risk.

1:30 – 4:30 PM


The top candidates in the security industry are referred to as “A-Players”; whether sales-focused to bring in business or technically-driven for operational roles, these individuals are in high demand, sought after and recruited by the very best security integration firms today. These standards are critical to the continued success of integrators in our industry! Are you preparing yourself to be in-demand talent? Do you know how to identify the very best security integration companies in the market as your home for continued career growth? Learn what you should be doing to strategically develop your expertise and ensure longevity for your organization.

Learning Objectives:
1. Establish the fundamental problems exist in our market and how they might be resolved.
2. Discern the ways thought leadership has used data to determine how the market has evolved.
3. Gather specific market examples to achieve improved operations and profitability.

2:45 – 3:45 PM


Disruption in the security risk landscape demands new leadership strategies to be relevant and effective for your organization. Are you prepared for the onslaught of additional threats from new technologies, new skills needed in the workforce and the increased cooperation needed between security and all facets of the organization? Join security industry veterans as they bring together leading global security practitioners redrawing the role of security within their organizations as they debate what and who will influence the opportunities and challenges ahead.

Learning Objectives:
1. Define ERM and evaluate the kind of protection needed for your enterprise.
2. Gain insights from panels on how the boundaries of security are being redrawn to create new value and redefine the security industry.

2:45 – 3:45 PM

Case Study: Rolling Out Business Intelligence with Superior ROI

Retailer Murphy USA is in the midst of a planned nationwide deployment of intelligent surveillance systems at 1,344 convenience store locations across 32 states. The new systems are comprised of IP and hybrid appliances, cameras and business intelligence software integrated into a customized solution. Discover how Murphy USA adopted a strategic approach to surveillance system usage and organizational accountability and efficiencies. In partnership with their systems integrator, they designed a solution that integrates POS, cameras, audio, analytics, time and attendance that will utilize the best-in-business intelligence software pulling data into an easy-to-use dashboard accessible anywhere users have an Internet connection. Ultimately, the goal is to have all organization departments utilize system data to improve operational efficiencies. Hear how the flexibility of the design, combined with mobile accessibility and the hybrid IP and analog capabilities were compelling selling points for the solution.

Learning Objectives:
1. Discover best practices for a year-long loss prevention system deployment to 1300+ retail locations.
2. Determine state-of-the art business intelligence software capabilities and measurable benefits across the retail organization.
3. Gather specific market examples to achieve improved operations and profitability.

4:00 – 5:00 PM

How to Implement a Life Cycle Management Program

Many organizations have come to the realization that physical security systems require the same level of management and maintenance as any server-based system. The complexity of integrations between software platforms, legacy and newer hardware and edge-devices in the field create an environment that is prone to outages if left alone. A life cycle management program is the best way to ensure longevity of systems, limit outages and their impact, and to have a budgetary plan this year and 3-5 years down the road. These questions and more will be answered in this presentation by panelists with first-hand experience.

Learning Objectives:
1. Determine the elements to implement a LCM program.
2. Discern the initial and ongoing steps necessary to effectively manage and maintain integrated systems.
3. Establish the impact on network and information security and ensure longevity for your organization.

4:00 – 5:00 PM

State of the Security Industry and Its Future

Join recognized security industry leaders as they provide their candid opinions on what they think the state of the security industry is now and what they feel the future will hold. They will debate the challenges and opportunities that lie ahead, identify evolutions driving the market now and address the key problems that need still need to be solved. Attend this session for a look into the future and what it will take not only to survive, but to thrive.

Learning Objectives:
1. Establish the fundamental problems exist in our market and how they might be resolved.
2. Discern the ways thought leadership has used data to determine how the market has evolved.
3. Discover opportunities that will help shape the future of the industry.
SIA EDUCATION @ISCEXWEST

Wednesday, April 6

7:30 – 8:30 AM
CCTV 101: The Basics and Beyond

Whether you’re a novice or veteran of CCTV system design and structure, this session is for you. Industry expert, Charlie R. Pierce will lead you through the needs and requirements of proper system design. Review the ‘how’s and why’s’ of proper application to determine how to present the best security solution for clients. This is an opportunity to understand the evolution of analog and IP structures: differentiating between putting a camera on a wall and developing useful, flexible and profitable solutions that provide long-term value.

Learning Objectives:
1. Differentiate remote site monitoring technologies and techniques.
2. Evaluate new technologies.
3. Apply the technology that is the best fit for an organization or project.

7:30 – 8:30 AM
Integrators Meeting the Challenge

Integrators today face an array of challenging business and technical issues. Product technologies continue to evolve on multiple fronts from video-related to communications to analytics and big data to cloud-based services. Overcoming these challenges are aspects of cyber threats. This presentation will feature representatives from system integrators discussing how they dealt with selected technical challenges. The challenges discussed will include IT technology, technical training, emerging technologies, cyber security, cloud services implementation and others.

Learning Objectives:
1. List actionable steps to address common technical challenges that may confront integrators.
2. Describe new problem solving methods and resources relevant to technology issues.
3. Identify new or emerging challenges integrator may face, based on experiences of peer companies.

8:45 – 9:45 AM
SIGNATURE SERIES SESSION

Lights! Camera! Action! How Paramount Pictures Delivers Enhanced Safety and Global Security While Driving Operational Efficiency and Sustainable ROI

This session open to all badgeholders!

Paramount Pictures is America’s oldest-running movie studio and has brought us many successful movies throughout the years, including “The Godfather,” “Indiana Jones”, and “Transformers.” Upholding the highest standards of business behavior and standards, Paramount also holds its global security operations in the highest regard, deploying some of the best and most innovative solutions. Paramount continues to make the safety and security of its employees, partners and visitors a top priority along with the security of its props, equipment and highly valuable film content worth millions of dollars. Additionally, Paramount sought to ensure business continuity in the face of ever-changing threats, along with a high level of operational efficiency for its global business. Add to that the need for a sustainable return on investment. The security, IT and management departments at Paramount know they needed to expand the role of the company’s private command center beyond the monitoring of only its production lots.

In this session, representatives from three departments within Paramount Pictures will address the security and business continuity needs of their demanding business, how they handle day-to-day operations and how they are achieving their goals of operational efficiency in a global market.

Learning Objectives:
1. Understand how business continuity and ROI go hand-in-hand.
2. Learn how large organizations handle the safety and security of assets and people throughout the globe on one easy-to-use interface that combines a number of life safety and security systems.
3. Recognize the value in achieving situational awareness for a global company.

10:00 – 11:00 AM
Keeping the Backend Up: Operational, Policy, and Technology Considerations for Managing IoT

The Internet of Things (IoT), is leaving end users across the public safety spectrum, literally awash in a sea of data. Security managers and public safety administrators currently operate a range of sensor systems that provide massive streams of information. This data offers operational opportunity and reward but also carries with it risk. How data is stored, who has access to it, can also have a range of legal and policy implications for an organization. This panel of legal, operational, and technology professionals will look at the developing IoT environment and discuss practical tools to manage the people, processes and technology issues present in the IoT environment.

Learning Objectives:
1. Review the operational, legal and technical tools available to help manage the IoT dilemma.
2. Learn how large organizations handle the safety and security of assets and people throughout the globe on one easy-to-use interface that combines a number of life safety and security systems.
3. Hear examples of IoT issues confronted by organizations and tools used to confront and mitigate concerns and challenges.

Global Security While Driving Operational Efficiency and Sustainable ROI

This presentation will explore the highly regulated environment and security requirements of medical marijuana facilities. The subjects of crime and loss prevention, physical security, and systems integrators will provide participants with the knowledge necessary to help them understand the field of security as it applies to medical marijuana facilities. Participants will be provided with intelligence to navigate the highly regulated environment of medical marijuana facilities, enabling them to create a security plan based on initiatives utilizing the comprehensive use of security technology.

Learning Objectives:
1. Differentiate the highly regulated environment of medical marijuana facilities—from governance to regulatory requirements and business initiatives.
2. Create a security plan for facilities based on security requirements and business initiatives.
3. Discern the comprehensive use of security technology necessary to stay in compliance with state and Federal laws.

Efficiency and Sustainable ROI

In today’s world, if a crime is committed, there is a good chance that there will be digital evidence associated with it. How will your video system be affected if witnesses to one of the many different types of crime, such as violent, white collar, or cybersecurity? If you suddenly find your security system behind “crime scene” tape, is your security staff educated in evidentiary procedures that prevent the loss of vital evidence, while keeping your video system functioning? Determine steps on how your IP video system may be affected by crimes that require involvement with different levels of law enforcement. If your organization becomes a target of cybercrime, you need to know how your video system be an accomplice to the crime or remain immune to its effects.

Learning Objectives:
1. Establish evidence recovery procedures based on event type and jurisdiction.
2. Validate the authenticity of system digital video.
3. Discern insights to audit the integrity of video system and components.

Clarifying Evidentiary Procedures for Digital Video and Admissibility

1. Review the basics of IP and analog cameras to determine the best solution for end-user conditions.
2. Discern tactics to bring video applications into modern solutions.
3. Create approach to drive application use and technology requirements for client solutions.

1. Identify new or emerging challenges integrator may face, with the knowledge necessary to help them understand the field of security as it applies to medical marijuana facilities.
2. Describe new problem solving methods and resources relevant to technology issues.
3. Discern insights to audit the integrity of video system and components.
Learning Objectives:
1. Identify the 12 disruptive technologies listed in the 2013 McKinsey Global Institute report.
2. Review how the technologies are affecting the security industry.
3. Create a plan of action for companies to implement a strategy to embrace these technologies.

10:00 – 11:00 AM
Have We Over Technologized the Video Surveillance Industry?
The CCTV industry has grown immensely over the past few decades. The advent of IP-based video and analytics have influenced the widespread use of video surveillance globally. But are we missing the “invisible gorilla”? Have camera systems become so much a part of our lives that they are no longer seen as a deterrent to crime? Think about the impact of mobile phone video on the physical security industry and law enforcement. Has video surveillance become just a reactive tool that documents crime without mitigating the risks proactively? Understanding the condition of “inattentive blindness” can impact how we design our surveillance systems. Technology without policy and procedures has the potential to expose organizations to more risk than it mitigates.

Learning Objectives:
1. Review how the CCTV Industry has evolved to where it is today.
2. Determine the concept of inattentive blindness and surveillance system design.
3. Recognize the impact that mobile phone video is having on the physical security industry and law enforcement.

11:15 AM – 12:15 PM
Countering the Threat of Drones
The proliferation of cheap drones UAVs are exposing gaps in perimeter security at such locations as the US Capitol, prisons, athletic events and critical facilities. This session covers the use of various technologies, such as radar, acoustic sensors and thermal and optical cameras to plug those gaps. These different sensor technologies will be compared to each other and the proper use of each particular technology discussed. Practical examples will be reviewed along with lessons learned from those installations.

Learning Objectives:
1. Contrast detection technology to the type of environment of operation and threat.
2. Discern the pros and cons of radar, acoustic and thermal detection technologies.
3. Gain insights for proper counter UAV detection and response systems.

1:45 – 2:45 PM
End to End Best Practices in Systems Integration
As the IoT affects the professional security industry, users’ demands for smarter and better integrated technologies will continue to evolve. Leading manufacturers/suppliers are already working to develop strategies, best practices and product protocols to ease integration and provide new, improved cross-functional capabilities. This presentation assembles a unique panel of industry leaders, representing a wide range of each particular technology discussed. Practical examples will be reviewed along with lessons learned from those installations.

Learning Objectives:
1. Discover how video surveillance has a large impact on elements outside of physical security, including analytics and business intelligence.
2. Compare and contrast the pros and cons of using 360-degree video surveillance cameras, along with the difference between different types of the cameras.
3. Recognize how 360-degree cameras can be leveraged for enhanced situational awareness.

10:00 – 11:00 AM
Wearable Cameras for Law Enforcement: The Challenging Dilemma
Body-worn cameras are being adopted by law enforcement agencies across America on a daily basis. Yet many states have yet to approve them for use. Many municipalities are waiting for their state’s attorney general to establish policies for body-worn video B/WV and some police departments are not supportive. Funding is yet to be identified. While it seems a foregone conclusion that body-worn video will be widely adopted, it is a matter of time. Join us for a fascinating and topical discussion on the issues facing B/WV adoption and deployment.

Learning Objectives:
1. Describe the five major body-worn camera use policies in debate at this time.
2. Identify five key wearable camera features that are mandatory and the storage options that are regularly considered.
3. Explain the key challenges facing police over body-worn video.

11:15 AM – 12:15 PM
Taking a Full Cycle Approach to CCTV Deployment
The installation of a CCTV system can be expensive and time consuming, therefore it is important to understand the full scope of implementing a CCTV system from start to finish. This session will review three key stages of the process: planning, determining technical considerations, and post-installation. Without complete understanding of an organization’s network, software, etc. an integrator may place themselves, as well as the project at risk. Determine how taking all technical considerations into account is vital to a CCTV system’s success.

Learning Objectives:
1. Establish technical considerations prior to implementation of a CCTV project.
2. Navigate the pitfalls that may lead to failed CCTV rollouts.
3. Adopt steps towards long-term success of implementation for CCTV solutions.

11:15 AM – 12:15 PM
The Convergence of Physical and Cyber Security: Recognizing the Readiness of IP-based Systems
Physical and cyber attackers have more sophisticated tools and understanding of network-based systems than ever before, shining a spotlight on the vulnerabilities of security implementations. This session will provide an overview of the 4 levels of physical security threats beyond perimeter, boundary and volumetric security, and present an innovative comparison to their cybersecurity counterparts. Detect methods of how to determine cyber-security readiness of video, access control and other systems, including a list of essential certifications, key elements of vendor compliance and testing procedures, and how to evaluate a vendor’s ongoing update program.

Learning Objectives:
1. Explain how network-based systems can be protected against cyber security threats and how to communicate these measures to your customers.
2. Determine how to implement security policies and procedures at the site level.
3. Review a list of qualifications for products and vendors when evaluating systems and the importance of third party testing for certain certifications.
SIA EDUCATION @ HOWEST

11:15 AM – 12:15 PM
The Growing Need for Mass Notification and Emergency Communications

Today, MNEC systems have grown to protect us against more than just fires. These systems alert and provide us with critical information and directions to follow during dangerous weather, acts of terrorism or other hazardous events. To reach 100% of occupants, these messages must integrate across multiple platforms and include a complete range of communication methods, both visual and auditory. The growing need for mass notification emergency communication systems is predicated on changes to building code and a belief that organizations need to provide these safety messages to building occupants and employees. For the security and system integrator, MNEC opens the door for additional value delivered to end users. For facility staff, understanding the key criteria for consideration in system design is imperative to implementing the right system for their facility.

Learning Objectives:
1. Identify specific codes that are generating awareness of Mass Notification Emergency Communication (MNEC) systems.
2. Define the critical criteria required for the successful design and implementation of any mass notification system design.
3. Articulate the complex aspects of system integration and determine a holistic approach when you are implementing a mass notification system.

12:30 – 1:30 PM
Solving the VMS Searchability Problem

Although video is simply data, it’s the one kind of data that no one—not even a tech genius at the best search engine company—has figured out how to index and search in a meaningful way. Video is only discoverable based on information that is manually added to the file, such as titles, descriptions, creator names and tags. Anything not noted is essentially invisible to a search engine. This problem is amplified in security applications, where video needs to be discoverable without any added text. Yes, video management systems (VMS) make large amounts of video searchable to a certain extent, particularly using timeline searches. However, that requires users to know when an incident occurred. The greater the possible time range, the more video there is to “hunt and peck” through looking for suspects or other important data. This session will cover video’s current “searchability” problem and what leading VMS providers are doing to improve discoverability. End user case studies will illustrate how VMS can now search and deliver specific data buried in vast amounts of video content.

Learning Objectives:
1. Identify three reasons why video data is different from other types of data.
2. Explain the technological advances that are improving VMS search capabilities.
3. Apply these advanced search options in new and existing security and surveillance installations.

12:30 – 1:30 PM
The Internet of Home: Next Generation Security and Smart Home Control

Adoption of smart home technology has gained greater traction for end-users in recent times. What are the larger market forces driving the IoT and the impact to the security industry in general? Hear perspectives from a global IoT infrastructure chip manufacturer, a software cloud service provider and leading security and related service providers as they discuss next generation platforms and services. The ecosystem of open and propriety systems and the end user experience will also be discussed. Gain insights into the next five years of IoT and connectivity.

Learning Objectives:
1. Examine how security and smart technology work together to provide a single, easy-to-use solution.
2. Determine methods to configure an expandable and upgradeable security and smart home system for any user.
3. Assess how today’s security and smart home systems can significantly reduce the cost of truck rolls, support calls, and service requests.

12:30 – 1:30 PM
Preparing for Physical Security Requirements of CIP-014: Designing a Sustainable Early Warning System

Recent attacks on utility substations, such as the one on PG&E Corp.’s Metcalf substation in 2013, have attracted the scrutiny of the media and exposed alarming physical vulnerabilities in the national power grid. Utility substations are inherently easy targets because they are often unmanned and in open, isolated locations. Despite advancements in security sensor and analytics technology, they’re often secured with nothing more than a chain-link fence and padlock. In response to these attacks, the North American Reliability Corp. (NERC) is developing a new set of security requirements (CIP-014-1) for substations to effectively deter, detect, delay, assess, communicate and respond to physical security threats. Beginning in 2017, substations will be expected to meet these operational and procedural requirements or face strict noncompliance fees that can reach as high as $1 million per day of violation. This session will explain a three-pronged approach involving perimeter intrusion detection, video management, and access control to help substations prepare for these ambitious new standards.

Learning Objectives:
1. Review the CIP-014 regulations to determine their impact on U.S. substations.
2. Evaluate the requirements of CIP-014 in relation to their own security systems and capabilities.
3. Assess security systems to integrate and meet the many compliance demands of CIP-014, ultimately avoiding harsh penalties and designing a more secure grid.

12:30 – 1:30 PM
Camera Apps Usher in a New Era in Surveillance System Design

There are many benefits offered with new and advanced IP video surveillance cameras, such as the ability to easily customize devices with third party apps. This presentation will focus on how apps have the potential to change the landscape in video surveillance system design and implementation by providing the ability to customize individual cameras with the specific functionality desired for every specific camera location. Session attendees will discover how camera apps not only increase functionality but also deliver savings on a system-wide scale.

Learning Objectives:
1. Compare differences between camera apps and conventional applications, such as license plate recognition.
2. Examine integrated edge solutions to review how integrators can provide new opportunities to add value to their design/builds.
3. Recognize how camera-based apps allow end users to customize their video surveillance systems with improved performance and cost-efficiency with new levels of ROI.
Thursday, April 7

7:30 – 8:30 AM
Access Control Vulnerability and Interoperability: Improving the Reader-to-Panel Connection

When it comes to gatekeeping, a common mistake is assuming encrypted ID cards are all it takes to keep the bad guys out. Unfortunately, the last inch of wire can compromise an access control system. SIA’s Open Supervised Device Protocol (OSDP) both standardizes the reader-panel connection and secures it. Session attendees will review how to physically wire an OSDP connection, and get a first-hand look at the inherent security flaws in Wiegand connections. Participants will also have a chance to assess their own systems for vulnerabilities and connectivity capabilities.

Learning Objectives:
1. Distinguish the benefits of migrating from legacy access control protocols to SIA’s OSDP standard.
2. Review the process to physically wire OSDP connections, configure panels and readers, and identify the associated component parts.
3. Identify how to address security vulnerabilities by implementing OSDP Secure Channel features in new and retrofit installations.

7:30 – 8:30 AM
Impact of Enterprise Security Risk Assessments on Integrators & Manufacturers

What exactly does a risk assessment mean to the integrator and manufacturer community? So often risk assessments are overlooked and not received as an essential piece of the project process. Collaboration with each of the essential elements of the business from the installation and implementation of the solution to the overall operation get neglected resulting in lost revenue and lack of actual fulfillment of what the customer actually needs. Ensuring manufacturers and integrators are interrelated in the overall process ensures that at the end of the day, the customer gets exactly what is needed and prescribed. Session attendees will review the procedure to prepare action plans and gain insights to recommend appropriate product and solutions as well as formulate realistic budgets so they are seen as a value-added resource. Participants will also have a chance to assess their own systems for vulnerabilities and threats and vulnerabilities before attending this session.

Learning Objectives:
1. Examine the considerations, impacts, and issues that are solved when manufacturers and integrators utilize a risk assessment to its fullest potential.
2. Leverage and understand risk assessment findings to appropriately plan, prepare and budget for a well-designed and effective physical protection system (PPS).
3. Explore best and proven practices that will assist the manufacturers, integrators and security risk consultants fulfilling customer needs by understanding, deciphering and properly utilizing risk assessments.

7:30-8:30 AM
Perimeter Intruder Detection for Electrical Power Generation, Transmission and Distribution Facilities

This session will discuss the challenges electrical power generation and distribution companies are facing with respect to securing installations from sabotage, violence, terrorism and copper theft. Potential security solutions geared towards protecting the perimeter around these facilities will be discussed as well as technical and cost trade-offs. Case study data will be presented to illustrate current installations and international best practices.

Learning Objectives:
1. Examine issues utilities, nuclear facilities, dams, substations and solar farms face in securing perimeter areas.
2. Review technology options used by facilities to reduce incidences of theft and sabotage.
3. Explain industry best practices used to deal with threat detection in the U.S. and worldwide.

7:30 – 8:30 AM
Regulation through Litigation – Lessons from Recent Data Breach Lawsuits and Enforcement Actions

With almost daily news of data breaches, privacy and security have taken on a new level of importance. In the last few years, enforcement of various privacy laws, including the Health Insurance Portability and Accountability Act (HIPAA), the federal Communications Act and state data protection laws have skyrocketed, with the Office of Civil Rights, States’ Attorney’s General, the Federal Trade Commission, the Federal Communications Commission and private individuals all taking action. This session will describe the privacy and security regulatory landscape, use litigation and enforcement actions undertaken by the various regulators and plaintiffs firms to demonstrate risks, and discuss vendor best practices to mitigate compliance risks.

Learning Objectives:
1. Describe the common business and IT practices that create the highest amount of risks for vendors
2. Implement a strategy to further your business to minimize data privacy and security compliance risks
3. Evaluate whether internal processes and controls are in place to address the most frequently targeted issues by regulators and plaintiffs firms

7:30 – 9:00 AM
SALES WORKSHOP: Creating Fully Engaged Customers

After working so hard to get an appointment, how do you get your customer fully engaged? Today it is harder than ever. Not only is it difficult to differentiate your company from your competition, but your points of contact seem to be in continual crisis mode. In fact, panic and distraction has become the default mode. Unless you’re able to get sales associates to shift out of their default mode so that they focus on your and the value you bring, you’ll just become another security sales person and might get a call to bid on a job in the future. Maybe in this session, attendees will work on the most effective game plan to dominate every sales call. With practical and hands-on exercises attendees gain detailed ideas from the preparation through the initial hand shake and the closing of the sales call.

Learning Objectives:
1. Prepare for every sales call in a unique and meaningful way that is relevant for today’s end-user.
2. Develop methods to shift your customer from their distracting thoughts of other tasks and projects to being fully attentive.
3. Discern how to position yourself as the authority, while disarming your customer.
4. Create a plan to close the sales call with confidence and impressive tone.

7:30 AM – 4:30 PM
FULL DAY WORKSHOP
WORKSHOP: Critical Thinking for the Security Professional

This unique workshop provides context on critical conversations with clients and coaches participants on how to think through problems in a systematic manner. Through interactive exercises, attendees will create concrete steps to experience increased sales and project profit margins while mastering solutions that accurately meet customer expectations on initial deployment. Gain insights to new thought processes which can be applied to delivering successful security projects to clients.

Learning Objectives:
1. Develop an action plan for increased confidence for critical conversations with clients.
2. Define problems more effectively so they can be clearly communicated to others inside and outside the organization.
3. Discern the thought process of a systematic assessment.
4. Create and execute a project plan that meets the expectations of customers, enlisting buy-in to generate full sign off from all stakeholders on projects.

8:45 – 9:45 AM
SIGNATURE SERIES SESSION
If You Only Knew What Hackers Can Do

With one in two organizations experiencing a serious security breach each year, and 94% of those breaches occurring in organizations with firewalls and anti-virus software in place, it is clear that legacy security solutions are no longer effective. Hackers are also developing new attacks through search engine optimization, which lists their malicious websites at the top of search engine results, and are also dispatching malware through messages on social networks. As cyber-attacks become more sophisticated and as the boundaries of infrastructure have become almost nonexistent with the onset of the cloud, mobile devices and big data, it is important to understand the different types of attackers and the techniques they use.

Learning Objectives:
1. Gain insight into the latest cyber intelligence reports as applicable to Data Center Resilience.
2. Define how converged logical and physical access control can alert on behavior and even alert on keyboard entry.
3. Recognize how to use cyber intelligence and protect yourself from attacks.
Learning Objectives:
1. Review methods to employ a private cloud structure in your environment to assure digital evidence is protected.
2. Develop an economical long term retention plan that includes-tiering your mobile or fixed camera content on multiple storage mediums.
3. Examine and learn to differentiate the cost benefits of storing digital evidence in a private cloud vs. public cloud.

10:00 – 10:30 AM
BACK BY POPULAR DEMAND
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 case law 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. Identify current problems with your contracts.
2. Develop a working knowledge of current laws affecting your contracts.
3. Correct your contracts so that they are more likely to be enforced.

10:00 – 11:00 AM
New Technologies for IP Surveillance Video Retention

As surveillance applications increase the number of cameras in their environment, and camera quality further enhances (resolution and frame rates), storage requirements grow exponentially. Add lengthening retention requirements to the mix and those storage requirements become overwhelming. It is essential to employ a solution that has the capability to safely and affordably retain video for any retention term. New technology has enabled surveillance environments to cost effectively store IP surveillance video utilizing long term, optimized, deep storage. Video from mobile or fixed cameras can now be archived to scalable disk and tape (LTO and T2S) technology via a simple cloud-like (S3) interface that integrates with cloud storage VMS providers and camera manufacturers. This private cloud infrastructure provides organizations an alternative to storing digital evidence on costly, public cloud options and makes retaining IP video economical and reliable.

Learning Objectives:
1. Review process to use analytics to effectively mitigate risks to optimize security and drive compliance in a mobile ecosystem.
2. Assess the privacy and security options for provisioning and managing identities throughout their lifecycle in the cloud and across different and/or multiple smart devices.
3. Identify contextual options for establishing trust for transactions on mobile devices used to access doors, critical data, cloud applications and other use cases.

11:15 AM – 12:15 PM
Cyber Security in Mobile Devices

As mobile devices proliferate in your organization and as your users migrate more and more of their activities onto smart phones and tablets, how do you manage compliance in the cyber and physical world? Users are reading email on their phones, accessing secure web sites using tablets, and in advanced scenarios using credentials in their phones to unlock doors and logon to computers. To comply with internal and externally-mandated policies, it is essential to manage the identities and associated credentials used. Hear about the mobile ecosystem and how the different components work together to secure access. Primary use cases will be used to illustrate the need for and mechanics to deliver compliance. The concept of an “Identity Perimeter” will be introduced and its importance for compliance will be explained.
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-at-materials labor to ensure a considerable increase in profitability.

Learning Objectives:
1. Explain the evolving IoT landscape.
2. Gain insight into how IoT will continue to impact and change the world in which we live.
3. Recognize IoT’s global impact and how it will affect the industry in the future.

Learning Objectives:
1. Prepare for every sales call in a unique and meaningful way that is relevant for today’s end-user.
2. Develop methods to shift your customer from their distracting thoughts of other tasks and projects to being fully attentive.
3. Discern how to position yourself as the authority, while disarming your customer.
4. Create a plan to close the sales call with a confident and impressive tone.

Learning Objectives:
1. Evaluate the value proposition of using biometric technology for large venues.
2. Define the key characteristics of touchless biometrics and how to overcome the challenges posed by this technology.
3. Apply best practices for configuration, system architecture, and demonstrate ROI as witnessed in successful implementations.

Learning Objectives:
1. Discover how open-architecture security systems allow venues to implement multi-sensor cameras to enhance the technology for a maximum return on investment.
2. Recognize the top deterrents to campus video surveillance and the driving reasons that schools adopt video surveillance, their obstacles. Additionally, what is the most accepted view relative to single sensor panoramic, traditional fixed IP and PTZ cameras.
3. Develop a plan to better customize campus solutions, including the convergence of physical and logical access. Gain lessons learned from the perspectives of the integrator, end user and biometric specialist. Several biometric integration projects are examined, focusing on how the newest touchless biometric technologies—fingerprint, identification, and facial and iris recognition—can balance assured security with high throughput, and maintain an unintimidating user experience, especially in educational environments and venues where children are present.

Learning Objectives:
1. Review the value proposition of using biometric technology for large venues.
2. Define the key characteristics of touchless biometrics and how to overcome the challenges posed by this technology.
3. Apply best practices for configuration, system architecture, and demonstrate ROI as witnessed in successful implementations.

Learning Objectives:
1. Review 2015 survey findings on K-12 & university campuses regarding the current attitudes on campus use of video surveillance and the driving reasons that schools adopt video surveillance.
2. Recognize the top deterrents to campus video surveillance deployment, to better address them for individual campuses.
3. Develop a plan to better customize campus solutions based on knowing the need for real-time video availability for law enforcement, the ability for parents to review the video and the desired camera placement and retention length.

Learning Objectives:
1. Discuss how multi-sensor technology began, how it is evolving and why it is a security industry game changer.
2. Identify how multi-sensor cameras are saving installers time and money.
3. Identify the innovative ways integrators are leveraging the technology for a maximum return on investment.
4. Discover how an open-architecture security systems allows venues to implement multi-sensor cameras to provide the highest quality views and best vantage points.