The 2017 Vision for the Security Industry

Megatrends

SIA
SECURITY INDUSTRY ASSOCIATION

SNG™
SECURING NEW GROUND®

Validating Your Strategy

SECURING NEW GROUND® (SNG™) is where you go to gather information, meet with your peers and discuss essential matters with your channel partners in the security industry.

SNG is the key conference where you validate your business strategy by listening to what others are doing. More importantly, together everyone turns their eyes to the future to explore how new trends are shaping the industry. In fact, from surveying SNG attendees in the past, we have heard that many say this is the one conference where they heard something that they had never heard before.

And so the Security Industry Association (SIA) is pleased to provide you with this report, "Megatrends: The 2017 Vision for the Security Industry," as a mechanism for you to look into the year ahead to guide your business through the market forces that may affect you and your customers.

> “ 10 megatrends for the security industry to incorporate into your own planning

At SNG 2016, held Oct. 19-20 at the Grand Hyatt New York City, thought leaders and captains of industry gathered to exchange intelligence in a number of panels and networking sessions. This Megatrends report distills the essence of those exchanges into 10 megatrends for the security industry, and then places them into context for you to absorb and incorporate into your own planning in the year ahead.

We hope this guide, the first of its kind, will serve you well until SNG 2017, which will return to New York in October 2017. Meanwhile, please find more information about SNG, including presentation slides and photos, online at **www.securingnewground.com**.

Thank you for your support of SIA and SNG.

Very sincerely yours,
Denis Hébert
Chairman
SIA

INTRODUCTION

The Impact of Change

10 Megatrends Affecting Security

IT'S BEEN AN EXTREMELY EVENTFUL YEAR for the security industry, with activity continuing to align with ongoing developments and transformation of traditional technology sectors to new acumens and revenue streams. Some of the major trends propelling the industry:

- Big buys in mergers, acquisitions, lending and debt equity.
- Mobile technology and cloud computing proliferation.
- Cybersecurity threats and compromises arising from a vast array of integrated solutions.
- GSOC evolution to collaborative and cooperative risk assessment.
- The continued rise of the Internet of Things (IoT), data, analytics and artificial intelligence.
- Ongoing emergence of big and smart data.
- Transformation of the integrator, alarm dealer and monitoring channels to new services and revenue models.

These aren't separate, disparate trends. In fact, each plays a role upon the other. For example, the cloud is becoming foundational to many emerging security applications, including mobile credentialing involving Near Field and Bluetooth communications, with the IoT poised to come on strong as still another disruptive technology within the physical security space.

It's been a year that has all stakeholders in the industry—security executives, chief information officers, systems integrators, manufacturers and distributors—reexamining their roles, duties and technology development. It's been a time to reflect and plan how to affect additional change and positively add value to the global marketplace for security. The impact of this ongoing change: a transformation of physical security to a prominent, proactive leadership role guiding the safety and security of the global economy.

Many of these megatrends have been discussed in detail by Steven Van Till, President and CEO of Brivo and Chairman of SIA Standards. Van Till especially sees the IoT, mobile technology, data, social media and cloud computing as creating challenges, along with greater opportunity.

"We have the ability, with data, to exert more control than ever before," Van Till said. "The equipment and software for security has the capability to contribute to business process improvement, for example, analytics for people counting. Now, security can strengthen the operational processes of an organization, even when there is not a direct security event," he said. "Data is critical, "but it needs to be aggregated in such a way that providers can derive more direct value."

Securing New Ground, presented by the Security Industry Association, is the thought leadership for the new way of doing business in security. It's a discussion of trends and the impact of change. It's a roadmap for forging future success by all the stakeholders in a market that now encompasses much more than physical security and safety. ■

> ***"We have the ability, with data, to exert more control than ever before."***
>
> —Steven Van Till, Brivo

MEGATRENDS

STAFF

Denis Hébert
SIA Chairman of the Board
dhebert@securityindustry.org

Don Erickson
SIA CEO
derickson@securityindustry.org

Geoff Kohl
SIA Director of Marketing
gkohl@securityindustry.org

Mickey McCarter
SIA Communications Manager
mmccarter@securityindustry.org

Alain Taylor
SIA Associate Director of Membership & Events
ataylor@securityindustry.org

Kimberly Roberts
SIA Director of Education
kroberts@securityindustry.org

Kevin Murphy
SIA Director of Membership
kmurphy@securityindustry.org

Marc Benson
Associate Director of Membership
mbenson@securityindustry.org

Deborah O'Mara
DLO Communications
Author and Chief Researcher

Michelle Wandres
Production Design

—

Security Industry Association
8405 Colesville Road
Suite 500
Silver Spring, MD 20910
Main: 301-804-4700
Fax: 301-804-4701
www.securityindustry.org

SIA SECURITY INDUSTRY ASSOCIATION

SNG™ SECURING NEW GROUND®

Premier Sponsors

ASSA ABLOY

interlogix United Technologies

NVIDIA®

Lenel United Technologies

SIEMENS

Event Sponsors

ALLEGION™

Arecont Vision®

AXIS® COMMUNICATIONS

CapitalSource

DELL EMC

FLIR

G4S

Genetec

Geofeedia

Hanwha Techwin America

HIKVISION®

Imperial Capital®

KRATOS® PUBLIC SAFETY & SECURITY SOLUTIONS

LOUROE ELECTRONICS World Leader in Audio Monitoring Technology Since 1979

NORTEK SECURITY & CONTROL

PELCO by Schneider Electric

PREFtech

RAYMOND JAMES®

SECURITAS Electronic Security

SYNNEX CORPORATION

Industry Partners

ISC

GLOBAL SECURITY RISK MANAGEMENT ALLIANCE www.gsrma.net

Media Partners

re:ID Regarding ID Magazine

SDM New Directions for Security Systems & Integration

The Path to Greater Profits SD&I Security Dealer & Integrator

SECURITY SALES & INTEGRATION

SECURITY SOLUTIONS FOR ENABLING AND ASSURING BUSINESS

SECURITY SYSTEMS NEWS THE NEWSPAPER OF RECORD FOR THE SECURITY SYSTEM INTEGRATOR & INSTALLER

SECURITY TECHNOLOGY EXECUTIVE

SP&T News

EXECUTIVE TAKEAWAYS

Overheard at Securing New Ground 2016

“Security departments must engage asset owners early or you're doomed. You risk being over deployed. Security must move from an old enforcement mentality to **LEADING BUSINESS DOWN PATH OF RISK MANAGEMENT**."

—John Petruzzi Jr., Vice President, Enterprise Security Operations, Charter Communications

“A lot of folks are participating in IoT without being familiar with the security space, sometimes operating without context. But where IoT is concerned, **THE ADULTS HAVE NOW ENTERED THE ROOM** as companies like Allegion and Lenel Systems are solving IoT problems."

—Rob Martens, Vice President and Futurist, Allegion

“New business models have come from consumers installing equipment but engaging professional monitoring services. I know an integrator that coined the phrase **'DO IT WITH ME'** service rather than DIY."

—Duane Paulson, Senior Vice President Product and Market Development, Nortek Security & Control

“We don't have data lakes, rather **WE HAVE DATA PUDDLES**, as most individual security systems are still isolated. More data pooling will occur with wider adoption of cloud solutions."

—Steve Van Till, CEO, Brivo

“Let's not call it cybersecurity; let's call it **GOOD ENGINEERING**."

—Adam Firestone, Senior Vice President, Solutions Engineering, Secure Channels Inc.

“Sharing your strategic security plan with your suppliers could yield greater understanding of your long-term goals and concerns. **NO ONE HAS EVER ASKED ME** for my strategic security plan—although they should."

—Bonnie S. Michelman, Executive Director of Police, Security and Outside Services, Massachusetts General Hospital

“We need people who can read a room and who have **STRONG EMOTIONAL INTELLIGENCE**."

—Maureen S. Rush, Vice President for Public Safety, Superintendent of Penn Police, University of Pennsylvania

“That's the value of Big Data: **ONE MAN'S TRASH IS ANOTHER MAN'S TREASURE**."

—Jack Wu, CEO, Nightingale Security

“The New York Port Authority created a central chief security officer recently based on recommendations from The Chertoff Group. That has been helpful in coordinating police response from Port Authority **RATHER THAN DEALING WITH SEPARATE INDIVIDUAL LINES OF AUTHORITY**."

—George W. Anderson, Director of Security, World Trade Center, Port Authority of New York and New Jersey

“Robots are **SIMPLY IOT THAT IS MOBILE**. To make them useful, they require AI data analysis. Robots need small, discrete AI programs to analyze Big Data."

—Jack Wu, CEO, Nightingale Security

“There will be one billion cameras worldwide by 2020, yielding 30 billion inferences per second. **HUMANS ARE NOT CAPABLE OF ANALYZING** this volume of data. Deep learning already has improved identification accuracy as much as 4x human rates as of today."

—Deepu Talla, Vice President and General Manager, Tegra, NVIDIA

“**WE MARKET TO LIFE EVENTS**—new home, new career, marriage—as opposed to population segments. So we do not distinguish millennials from other buyers."

—Amy Kothari, President and CEO, My Alarm Center

“Companies should tie credentials together, tracking employees throughout the enterprise while also **PROVIDING MORE CONVENIENCE**."

—Allen Viner, Head of Physical Security and Security Administration, AIG

“Every few years, we see a multibillion dollar transaction in the security industry but to see **FOUR IN ONE YEAR IS UNPRECEDENTED**."

—John E. Mack III, Executive Vice President, Co-Head of Investment Banking, Head of M&A, Imperial Capital

“Although it may not always have felt like it, the security industry was **A NET BENEFICIARY OF INVESTMENT DURING THE RECESSION**."

—Alper Cetingok, Managing Director, Investment Banking, Co-Head, Security, Defense & Government Services Practice, Raymond James & Associates

The Internet of Things

Security for the industrial IoT revolution

THE INTERNET OF THINGS (IoT) continues to forge new integrations between a vast, ever-growing array of systems, sensors, devices and services. With unbridled connectivity of sensors to people, processes and things, once disparate systems, such as physical security, will be a critical part of the IoT.

The IoT is set to redefine every person, industry and vertical market, especially physical security and its practitioners. With it comes opportunities and challenges—especially how to defend open, non-proprietary systems and data points against compromise. For security executives and providers, the risks are real; the solutions still to be defined as technology becomes further entrenched.

> **“The inherent risks of IoT must be analyzed and understood. It’s coming at us as an industry with speed and velocity. The big question is: ‘How can we be better prepared?’”**
>
> —Jeff Spivey, Principal, Security Risk Management Inc.

Gartner Inc., Stamford, Conn., estimates that 5.5 million new devices are being connected to the internet every day, with the number to reach 6.4 billion by the close of 2016.

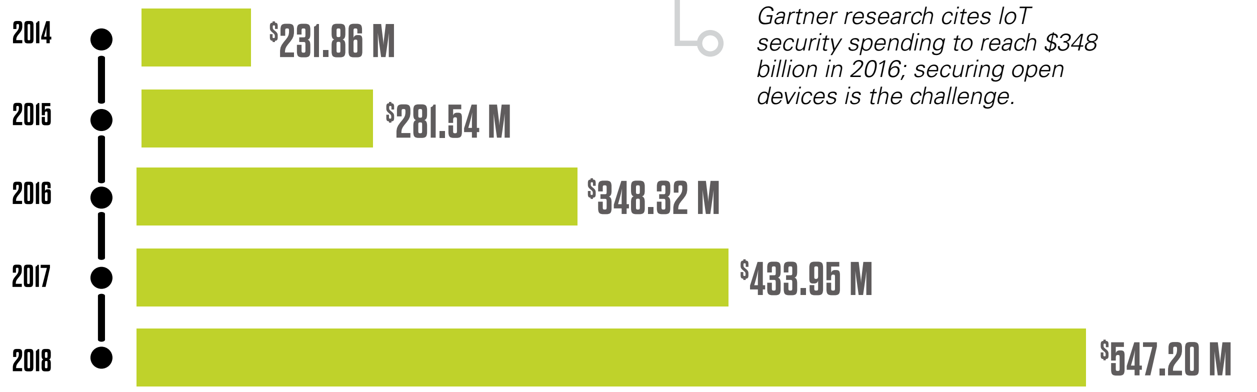
In 2015, the Federal Trade Commission (FTC) released the report, “Internet of Things: Privacy and Security in a Connected World,” focusing on data and privacy concerns with the ongoing implementation of connected devices. According to the FTC, experts estimate there will be some 50 billion connected devices by 2020. In the report, the FTC defines IoT as “devices or sensors—other than computers, smartphones, or tablets—that connect, communicate or transmit information with or between each other through the internet.”

Gartner further predicts by 2018 more than six billion connected things will be requesting support and through the same year, half the spending for IoT solutions will focus on integration. In addition, by 2020, more than 25 percent of identified attacks in enterprises will involve IoT, although IoT will account for less than 10 percent of IT security budgets.

The IoT is an opportunity to empower the industry to use data to drive better risk management solutions, even artificial intelligence. The entire realm of situational awareness continues to transition as intelligence is gleaned from new points, with this trend magnified by the IoT.

Protected properly, the IoT will bring more efficient processing and analysis of data, so security stakeholders can take advantage of a huge resource of intelligence to detect risks proactively, respond to situations in real-time and increase the efficiency of safety and security measures. ■

Worldwide IoT Security Spending Forecast



Gartner research cites IoT security spending to reach $348 billion in 2016; securing open devices is the challenge.

Source: Gartner (April 2016)

Cyberthreats and Compromise

A transformative model for proactive risk management

LET'S TALK POLITICS, BRIEFLY. The 2016 presidential debates focused highly on cybersecurity and threats, with each candidate talking about the magnitude of these potential incidents from malicious takeover or terrorism.

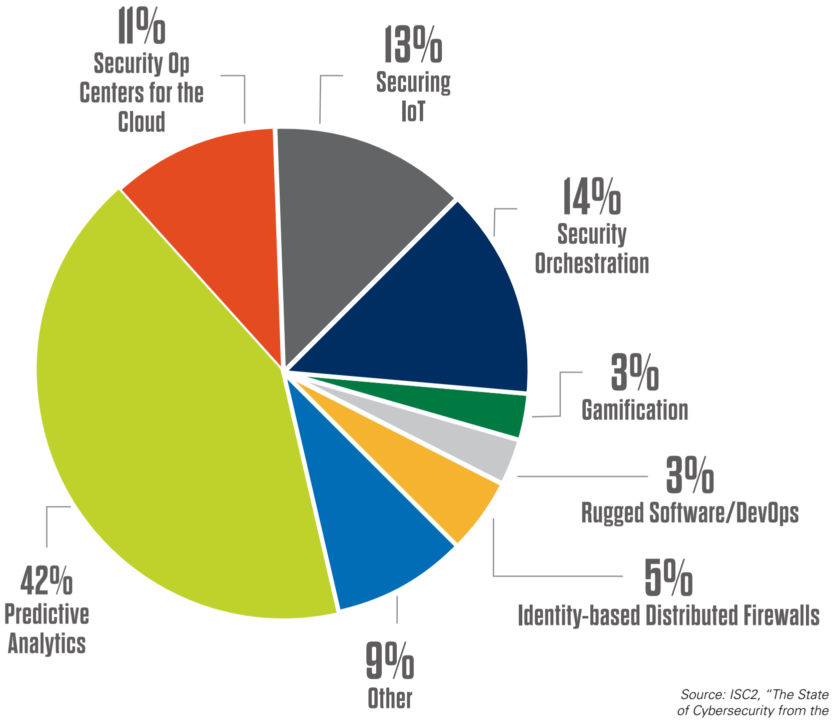
Politics over.

The vulnerability of the critical infrastructure was chronicled by the Wall Street Journal in a 2013 attack on PG&E's Metcalf facility near San Jose, California. Gunmen knocked out 17 transformers that help power Silicon Valley only narrowly averting a blackout, with the perpetrators never apprehended. The following year, the Federal Energy Regulatory Commission, which regulates the country's interstate power system, required utilities to protect their assets, including the use of cybersecurity measures.

The loss to business continuity can be astronomical and devastating. IBM and the Ponemon Institute, a privacy and information management research firm, conducted a study in 2016 in the United States that found the average consolidated total cost of a data breach grew from $3.8 million to $4 million.

In April 2016, the FBI and the Department of Homeland Security began warning infrastructure companies about the threat of cyberattacks on the U.S. power grid, following the attack on Ukraine's power infrastructure that left hundreds of thousands without power. Security researchers concluded the attack was carried out by Russian government hackers based on the type of malicious software, called BlackEnergy malware, which was detected in the incident.

Which is the most significant game-changing security technology or solution?



Source: ISC2, "The State of Cybersecurity from the Federal Cyber Executive Perspective"

With so much convergence between systems and technologies, cyberattacks can come from many fronts. Take the IoT for example: In 2015, HP reported that 70 percent of commonly used IoT devices are vulnerable to cyberattacks and breaches.

For the security practitioner, the goals are many and include having hardened products and processes; educating all stakeholders and systems integration companies; establishing cybersecurity and IT best practices; while balancing customer needs and desires for implementation. Manufacturers need to build resiliency into products during production, not as an afterthought. The security industry is focusing on prevention and detection—working to anticipate and prepare with predictive analysis of systems solutions. ■

> ***"The methods with which organizations protect their networks has shifted from being reactive to proactive through technology, big data and intelligence."***
>
> —Shawn Henry, President, Crowdstrike Services, and CSO, Crowdstrike

Smart and Big Data

Analytics and artificial intelligence boosts situational awareness

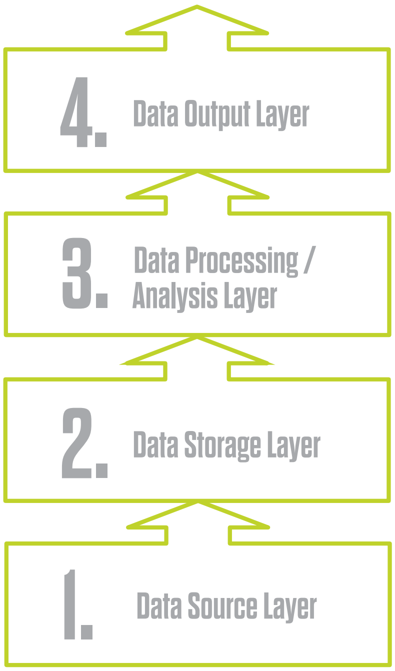
THE MORE INFORMATION, THE BETTER. Or so goes the story.

In physical security, pertinent information and data collection is the tie that binds. How do we gather all this data, and effectively sift through it to arise at the real-time information needed to address a threat prior to an actual loss or act of terrorism? How do we make it "smart" data that security can instantly put to use? For security practitioners, that's the goal at hand.

Big data brings huge benefits to businesses of all sizes. This layer is all about turning data into insights, arising to what we can adeptly refer to as smart data. Smart data is targeted information and specifics that provide valuable metrics and other criteria to effectively provide additional safety and security plans, processes and protocols. Cloud computing in particular has opened numerous options for using big data, as it means businesses can tap into this information without having to invest in massive on-site storage and data processing facilities. It's always at the ready, with an internet-connected device.

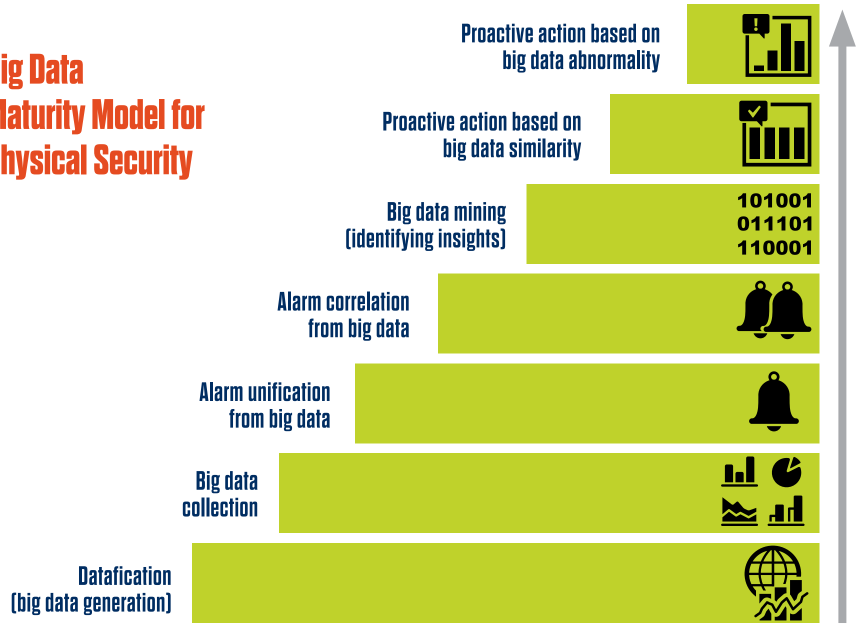
> ***"Organizations are drowning in data. How do you get the real information? It's a balancing act, with hardware, software and people components. Training, operational guidelines and benchmarking are needed."***
>
> —Ken Mills, Chief Technology Officer, Surveillance and Security, Dell EMC

4 Layers of Big Data



Source: Bernard Marr

Big Data Maturity Model for Physical Security


Proactive action based on big data abnormality
!
Proactive action based on big data similarity
✓
Big data mining (identifying insights)
101001
011101
110001
Alarm correlation from big data
Alarm unification from big data
Big data collection
Datafication (big data generation)

Source: Dr. Bob Banerjee

Making data work smarter

The security industry's mission is to use this information to become anticipatory and preventative. Customers, installation partners and stakeholders within an organization need to have an understanding of how data flows within the system, and not simply on the method to get the information, such as a user interface.

This is a monumental shift for the industry and needs to be prioritized. Once addressed, new opportunities will open for integrators to again be able to solve complex problems for the customers, adding to their value proposition. It requires ingenuity and innovation to deploy the right strategies to get the correct information quickly and easily digestible to enhance safety strategies. ■

MEGATREND 4

GSOC Evolution

Collaborative, cooperative and all-encompassing

A NEW DAY IS DAWNING in the evolution of the Global Security Operations Center (GSOC). What began as a method to address current issues, challenges and threats to the enterprise, employees and visitors is moving into an era of predictive analytics and proactive risk analysis—generated from systems, sensors, real-time location systems, social media and people, processes and technologies. GSOC takes many forms and is increasingly recognized as a necessity to support an enterprise's global business goals and operations.

> **“An effective GSOC necessitates an individualized approach for every enterprise client, determined by an in-depth analysis and ongoing assessment of threats, issues, challenges and possible past incidents.”**
>
> —Jasvir Gill, Founder and CEO, AlertEnterprise Inc.

Transformative and predictive

The GSOC is no longer strictly reactive. It continues to leverage a host of data, information, analytics, access control and other resources to provide advanced threat assessment and assistance. It leverages cloud computing, IT networking, video surveillance and compiles data not just in a resource housing information, but in a manner that allows it to be interpreted quickly by any user, at any time. Social media also plays a role, often determining where the bulk of people are located or communicating information and with specific directions emanating directly through these platforms so actions can be taken swiftly and pointedly. The GSOC has evolved from siloed operations to collaborative, cross communications from all stakeholders, law enforcement and first responders.

Situational awareness and risk mitigation take center stage. Historical and current data provide predictive analysis of developing situations. Today and in the future, the GSOC can be a better business enabler, avoiding catastrophic loss and protecting employees from potentially dangerous or threatening situations. ■

5 Critical Points for GSOC Transformation

1. Bridging the gap between system silos.
2. Predictive analytics from behavioral analysis.
3. Information and data from inside and outside the organization.
4. Integrating physical and IT security information.
5. Balancing mobile technology, privacy and security.

Transformation of Systems Integrators

Moving to managed services solutions and new revenue models

A FAMILIAR STORY CONTINUES TO PLAY OUT across the systems integration landscape. Big project revenues still exist, but can't sustain a company during an economic downturn or provide predictable, long-term revenue. For smaller projects, hardware margins have dwindled to single digits and competition is coming from every front—including the self-monitoring and DIY markets.

New recurring revenue models

Just like the IT provider of yesterday, the systems integration community is adjusting its business model, reexamining the way it gains customers. Companies are becoming total solution and service providers, focusing on convenience and an enhanced customer experience, providing proactive managed services that not only provide tangible, predictable recurring monthly revenue, but boost the value of the company through this attractive and sustainable model.

> ***"In the past, systems integration revenues were primarily project based. Research confirms systems integrators are moving more toward a recurring revenue model through offering service and maintenance contracts."***
>
> —Oliver Philippou, Senior Analyst, Technology, IHS Markit

The IoT, mobile technology, cloud computing and other megatrends are also positively affecting the systems integration community. There are more services to provide and the beauty of it all is that many of these services can be performed remotely—drastically reducing service costs and eliminating in many cases on-site field visits—and giving new confidence to consumers of just how valuable their contractors are to their homes and businesses as they provide 24/7 uptime and continual connectivity.

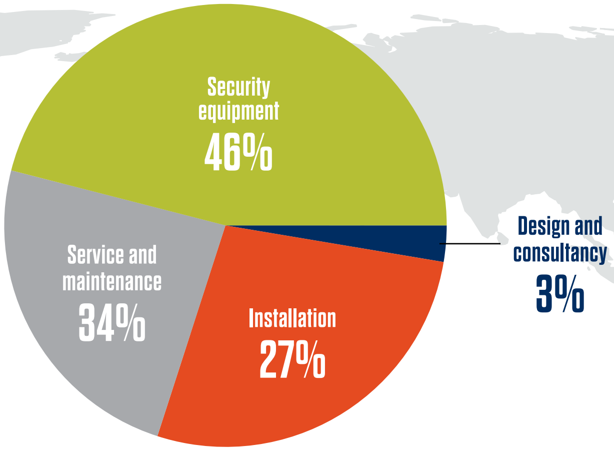
Revenue shines from service

Service and maintenance is being realized as a primary profit center by many systems integrators. The shift is notable and has been documented. A recent study by IHS Markit in London cites installation and maintenance as now comprising a strong overall part of the global market for security systems integration. IHS research predicts the services market, which includes design and consulting, installation and service and maintenance, as the fastest growing sector. The study shows service and maintenance accounted for 24 percent of the world market for security systems integration, a generous uptick from prior research.

In addition to making the company more stable with predictable cash flow, service also makes a customer stickier and more likely to stay with firms that provide a full array of services. The move to the IoT and additional data points and connectivity as well as increased system complexity is expected to continue to aid and assist this trend. ■

The world market for security systems integration

Global 2015 market size: $60.3 billion



Source: IHS

Return of Strategic Acquirors

Investment insights and private equity

FINANCIAL AND INVESTMENT COMMUNITIES have had their hands full the last several years, with an uber-active landscape and technology transformations bringing new, tangible value to both the installation and manufacturing sectors of the industry.

There are new entrants, startups and familiar faces boosting their companies with mergers and acquisitions and new infusions of cash. In the physical security industry, the combined equipment and services market was estimated to be $123.67 billion in 2015, according to IHS Markit and the Physical Security Equipment and Services Report. The research firm named Tyco International as the largest supplier to the equipment and services market in 2015, comprising 3.8 percent, followed by ADT, at 2.9 percent and the "biggest mover" as Hikvision at 2.5 percent. Further, the market share of the top 15 security equipment and services firms accounted for 21.4 percent of the equipment and services market in 2014, growing to 23.1 percent in 2015.

This research, however, does not include some of the big buys that occurred in 2016, most notably the merger of Tyco with Johnson Controls, the acquisition of Diebold's North American electronics security business by Securitas, the acquisition of ADT by Apollo Global Management and merger with Protection 1 and ASG Security.

> ***"For the security industry it was really a phenomenal year, featuring some of the largest transactions to take place in the history of the industry."***
>
> —John Mack, Executive Vice President and Managing Director, Imperial Capital

Making progress and heightening profitability

These recent transactions as well as others highlight the attractiveness of the market, the ability of participating companies to embrace new technologies and ways of doing business, continued commoditization and lower pricing of equipment and an emphasis on cloud computing, the connected home and building and the IoT. Remote video surveillance is clearly in vogue as well as new managed services, especially in commercial markets.

Fueled by private equity, the high volume of acquisitions in the past year marks the return of strategic acquirors in particular. It's expected 2017 and beyond to be highly active as well. ■

Security M&A Trends

Trend	Commentary	Example
Large-scale, landscape changing transactions	■ 2016 has seen a number of multi-billion dollar transactions that will have a material impact on the industry's competitive landscape. ■ Demonstrates conviction on the part of executives and financial investors in the fundamentals of the industry.	■ Protection 1 acquisition of ADT ■ Johnson Controls acquisition of Tyco ■ Universal Services of America merger with Allied Barton
Return of strategic acquirors	■ After a meaningful hiatus from the M&A landscape, strategic acquirors are back. ■ Several highly synergistic strategic transactions have already taken place in 2016 with several more in the works.	■ Alarm.com acquisition of Icontrol Networks (Connect and Piper business units) ■ OSI Systems acquisition of American Science & Engineering ■ Honeywell acquisitions of Xtralis and RSI
Increasing interest in security among financial acquirors	■ Represents continuation of trend observed over the last five years, in particular as it relates to new investors entering the industry. ■ Valuations remain strong, however concerns over sustainability of current levels growing.	■ Snow Phipps acquisition of Electric Guard Dog ■ LLR Partners acquisition of Eyewitness Surveillance

Source: Alper Cetingok, Managing Director, Co-Head of Security, Defense & Government Services, Raymond James

Mobile Technology

BYOD evolves into greater situational awareness and real-time presence

MOBILE TECHNOLOGY is taking its rightful place as the #1 access control credential. But it's also enabling greater safety and security, with enhanced situational awareness and the ability not only to control access but deeply authenticate individuals and provide real-time presence and location status which can aid significantly in emergency situations.

The smartphone is the control of choice of business users and consumers. It's highly unlikely for someone to lose this credential, making it reliable and convenient. Mobile applications and smartphone are an enabling technology. Manufacturers are building their business on the convenience and the ability for users to control systems, remotely program, view the protected premises via cameras and provide a significant amount of security and safety no matter how far they are from the protected premises. Soon, the smartphone will be the preferred access control credential, capable of providing two-factor authentication and encompassing biometrics for deeper security.

> ***"This is the first time in the history of physical security we have a vector to put applications in the hands of people coming and going to and from buildings. We had no interactivity prior with residents or tenants of buildings. We are putting critical apps in people's hands."***
>
> —Steven Van Till, CEO of Brivo and Chairman of SIA Standards

Unification with physical security

Mobile is a unifying technology. It provides real-time, location-based services/global positioning systems and includes social media connectivity. Analyzing mobile information and devising a comprehensive and cybersecurity plan takes a collaborative effort by the industry's stakeholders. Many institutions of higher learning are already embracing sophisticated communications technologies, such as mobile, video, cloud, wireless, social media and unified communications for campus safety and security and also to improve the learning experience in the classroom and throughout the campus—the business process improvement side of the equation.

The proliferation of mobile technology will drive the future direction of safety and security. The goal of the industry is to collaborate with all stakeholders to address and develop a plan that initiates and fosters more effective and connected communications. ■

92% +

adults have smart-phones, and mobile technology continues to proliferate the access control and intrusion markets.

Cloud Computing

An enabling technology for security and safety

ALTHOUGH THE SECURITY INDUSTRY may be lagging as far as adoption of cloud technologies—behind the IT sector, for example—we're gaining speed.

According to Gartner Inc., worldwide public cloud services market will grow some 17 percent in 2016, to total $208 billion, up from $178 billion in 2015. Gartner's research points to the highest growth from cloud infrastructure services or infrastructure as a service, projected to grow 42.8 percent in 2016. Cloud application services, known as software as a service, one of the largest segments in the global cloud services market, is expected to grow 21.7 percent in 2016 to reach 38.9 billion.

Many systems and services use the cloud for physical security, most prevalently access control but also physical security management of video surveillance, intrusion, and of course the connected building and home market.

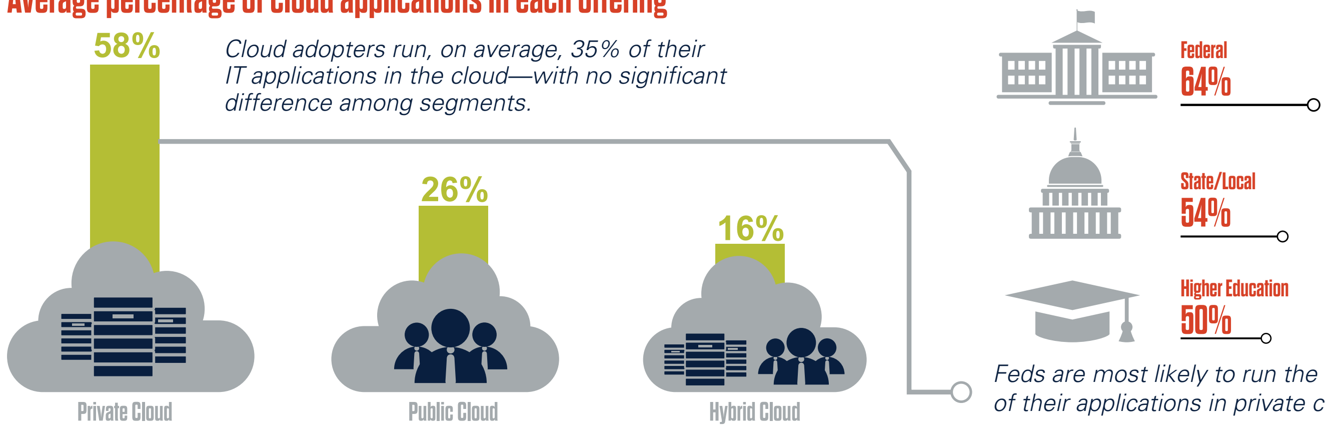
"Selling access control as a service (ACaaS) instead of just moving hardware and software packages adds value and predictable revenue streams to the systems solutions business, while providing substantial benefit to their customers who can move from large capital outlays for security to a monthly operating expense," said Denis Hébert, SIA Chairman of the Board and President of Feenics Inc. "I believe cloud-based subscription services for hosting physical access control in a true cloud environment, will be the number one change having a substantial impact on our industry."

> **"Cloud adopters are working to understand the rules of the road and want roadside assistance. To get in the fast lane to real cost savings, cloud adopters need clear migration strategies, appropriate cost models and need to prioritize the most critical cloud-ready apps."**
>
> —Milo Speranzo, Director, Strategy and Compliance, Avnet Government Solutions

Government entities climb on the cloud

According to *Destination Cloud: The Federal and SLED Cloud Journey*, a report released by MeriTalk, public sectors are rapidly adopting cloud computing, from police stations and state colleges to the nation's capital. Some 55 percent of cloud adopters are evaluating cloud solutions as part of their overall IT strategy and 45 percent looking at cloud solutions for a limited number of specific applications. These adopters report that cost savings is a key cloud driver: 65 percent of federal, 67 percent of state and local and 59 percent of higher education. MeriTalk's research cites improvements in productivity, customer services and cost savings as critical to the benefit of moving applications to the cloud. ■

Average percentage of cloud applications in each offering



Cloud adopters run, on average, 35% of their IT applications in the cloud—with no significant difference among segments.

Feds are most likely to run the bulk of their applications in private cloud:

Source: MeriTalk

MEGATREND 9

Social Media

Driving enhanced situational awareness and proactive emergency management

SOCIAL MEDIA HAS BECOME AN IDENTIFICATION TECHNOLOGY. With embedded location services, smartphone and social media users can be readily identified and locations pinpointed.

Integration bolsters situational awareness with real-time information emanating from social media posts and communications. It also delivers topic-trending information from Twitter. By monitoring many disparate systems, potential threats and trends can be identified, and that information can be delivered to facilities and security management.

> *“At Facebook, a big challenge for us is our open structure. Employees are encouraged to try new things and that brings risk to the organization. Executive residences are powered by the corporate network, so we focus on education to let people know what’s safe and what’s not.”*
>
> —Tim Wenzel, Residential Security and Special Projects Manager, Executive Protection, Facebook

Law enforcement and first responders use search engine optimization to look for key words cited in open and public Twitter feeds, for example: shooter, bombing, fire, rape. Because Twitter activity posted online is public and includes geo-locations based on the IP address of the person initiating the communication, security stakeholders can more accurately pinpoint the area of that communication and provide greater insight through deeper knowledge—the basis of situational awareness. Police departments also regularly search Facebook and Twitter to locate criminal suspects or get tips on their whereabouts.

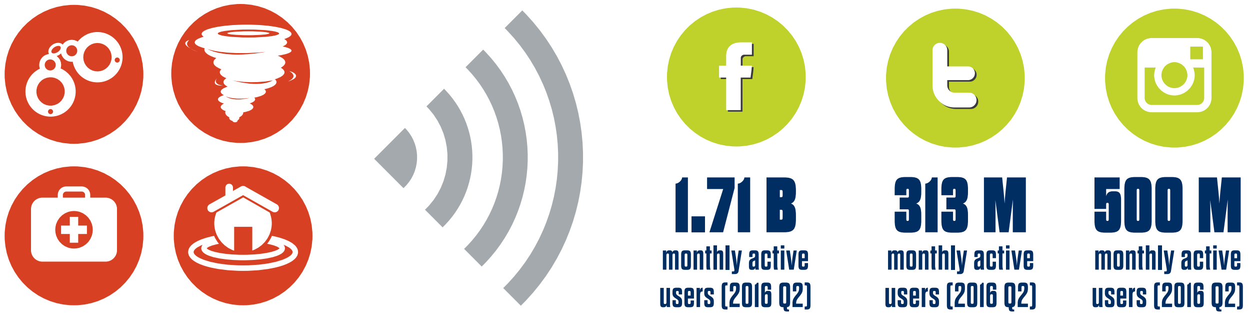
First responders are also leveraging geo-location services in these platforms and others to communicate disasters and emergencies. In June 2016, the Department of Homeland Security released “Using Social Media for Enhanced Situational Awareness and Decision Support.” In addition: *Hashtag Standards for Emergencies* was a Think Brief published recently by the United Nations Office for the Coordination of Humanitarian Affairs.

It’s an influencer, a disruptor, an enabler. It’s evolved to social identities, said Steven Van Till, CEO of Brivo and Chairman of SIA Standards. “Social media is emerging as a tool that can be used in different ways related to an emergency or security. Research suggests that people who lived in close-knit communities have better outcomes related to medical emergencies because they had people who could help them. Social media can be leveraged in a similar way.”

The risk side of the equation

Open architecture, mobility, BYOD and social media also bring new risks to an organization. It’s incumbent upon the security executive and practitioner to individually address and assimilate emerging technologies into asset protection planning. Incident management and continuity and compliance tools will continue to emerge, with security executives leading the charge. ■

Applying Homeland Security Scenarios to Social Media Platforms



MEGATREND 10

Do It With Me

The alarm dealer and monitoring segments move with the market

MONITORING AND A MOVEMENT TO RMR SERVICES continue to transform both central stations and dealer operations. There's new competition from every angle, including the self-monitoring, monitoring on demand and DIY markets. New entrants and start-ups see promise and dive in quickly. IT expertise is a necessity, not an afterthought.

Channels address challenges

Customers want convenience, in fact, demand it or they will go elsewhere. New monitoring options have emerged, giving customers the ability to decide when they want to monitor their systems and for what period of time—a month, weekend or even a day. Soon, they will have a virtual shopping cart of options in products and services to select online. The upside? Many of these customers are millennial, who may opt for more professionally installed systems as they age, or decide on long-term monitoring from their preferred provider as they gain new awareness of the indispensable role integrated systems play in their everyday lives.

Self-installed but professionally monitored systems are another way alarm dealers are embracing changing buying habits. Interactivity is key. Customers are looking for more value from their solutions and those who use their systems regularly are more likely to stay with their service providers.

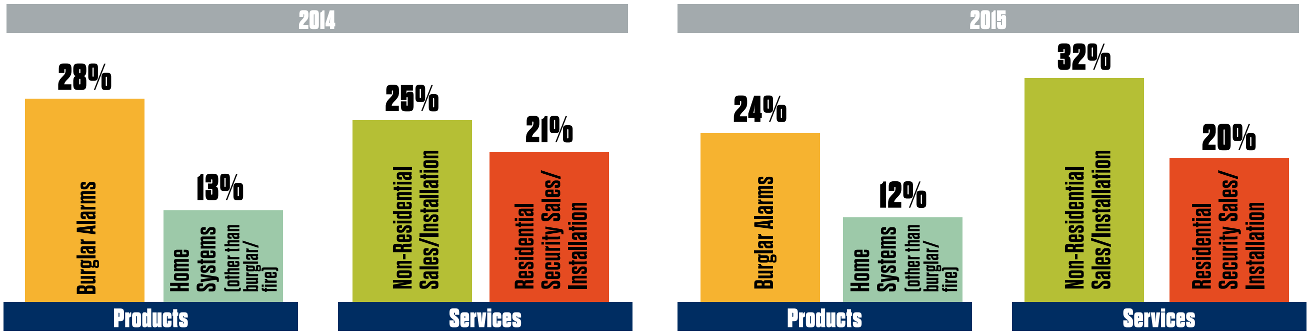
The scene cries for adaptation and companies continue to adjust their way of doing business. Integrating cloud-hosted video, access control and implementing mobile technology has made central monitoring stations competitive and ripe with renewed clout. Alarm dealers too have witnessed the transformation. Many have adopted progressive models that support DIY systems, with dealers stepping in to install them, assist with an installation gone awry, or service these components. They are embracing change and stepping solidly into the future with plans to continue to address a wildly fluid and diverse buying public, whether consumer or facilities manager.

> **“Alarm dealers are facing the largest and most rapidly changing environment they have seen in 25 to 30 years. It's not going to settle down any time soon. Those who embrace technology and change, while delivering to a 24/7 connected world, will do very well.”**
>
> —Tracy Larson, CEO, WeSuite

The value proposition still clearly revolves around security, but now, it's all about the connected system that can do more than turn intrusion detection on or off. ■

Alarm systems share of revenue by products and services

A recent shift in earnings may foretell a new trend in sales of products and services.



Source: SDM

SIA

SECURITY INDUSTRY ASSOCIATION

SNG™

Securing New Ground®