SECURITY MEGATRENDS™

THE 2018 VISION FOR THE SECURITY INDUSTRY

SIA
SECURITY INDUSTRY ASSOCIATION

SECURITY 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

KEVIN MURPHY
SIA Director of Membership
kmurphy@securityindustry.org

KIMBERLY ROBERTS
SIA Director of Education
kroberts@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

DEAR COLLEAGUES,

Thank you for a successful Securing New Ground (SNG) 2017 conference. SNG 2017 was one of the strongest and most engaging executive conferences in recent memory, providing all of us with strategic insight on current and future directions in the security domain. From this insight, the Security Industry Association (SIA) is proud to provide you with a compilation of the key trends discussed at SNG 2017, in this our second edition of the Security Megatrends report.

The only constant is change, and we hope Security Megatrends: A 2018 Vision for the Security Industry can help you navigate the inevitable. This report is developed as a companion to the SNG conference with executive takeaways and supplemental research to serve as a strategic sounding board for how megatrends, the prevailing market forces in the security industry, might affect your business. It is our hope that you derive from it some thoughts to guide your own strategic planning in the year ahead.

"WE ARE FORTUNATE TO GAIN SUCH INSIGHT FROM THE CALIBER OF MEMBERSHIP SIA ENJOYS, AS WELL AS THE QUALITY OF THE MANY CONTRIBUTORS TO SNG."

In this year's Security Megatrends, we distill these prevailing forces into a "Top 10" list, and look at where they are leading in the coming year. While we see recurring shifts that remain dominant, we peer into different aspects of trends like Cybersecurity, the Internet of Things, Big Data, Integration into Social Media and more to uncover where the discussions of these topics are heading in the C-suites of many companies.

Nothing similar to this report exists in our industry, and SIA is proud to provide this as a benefit to its members. We are fortunate to gain such insight from the caliber of membership SIA enjoys, as well as the quality of the many contributors to SNG.

We look forward to seeing you at SNG 2018! Keep tabs on registration and other details by visiting www.securingnewground.com.

Thank you for your support of SIA and SNG.

Sincerely,
Denis Hébert
Chairman, SIA

SIA SECURITY INDUSTRY ASSOCIATION

SNG™ SECURING NEW GROUND

THANK YOU

SIA THANKS ITS 2017 SNG SPONSORS.

ASSA ABLOY

SIEMENS

ALLEGION™

interlogix
United Technologies

LENEL
United Technologies

ANIXTER

Arecont Vision®
Leading the Way in Megapixel Video™

AXIS COMMUNICATIONS

CapitalSource

Convergint TECHNOLOGIES
Making a Daily Difference

alhua TECHNOLOGY

Dataminr

G4S

Genetec™

Hanwha Techwin America

HID

HIKVISION

Imperial Capital®

Johnson Controls

LOUROE ELECTRONICS
World Leader in Audio Monitoring Technology Since 1979

NORTEK SECURITY & CONTROL

Panasonic

PELCO
by Schneider Electric

RAYMOND JAMES®

STANLEY Security

INDUSTRY PARTNERS

ISC
INTERNATIONAL SECURITY CONFERENCE & EXPOSITION

GSRMA

MEDIA PARTNERS

SD&I

SDM

Security InfoWatch

SECURITY
FOR TODAY'S SECURITY PROFESSIONAL

SECURITY
SOLUTIONS FOR ENABLING AND ASSURING BUSINESS

SECURITY SYSTEMS NEWS

SECURITY TECHNOLOGY EXECUTIVE

EXECUTIVE TAKEAWAYS

OVERHEARD AT SECURING NEW GROUND 2017

SNG™
SECURING NEW GROUND®

"What is holding us back in the commercial world? **OUR CHALLENGE IS TO MAKE TECHNOLOGY EASIER TO DEPLOY**. The bar is going up with Nest and others as far as ease of use and that's been a challenge for us."

–Martin Huddart, President, Access and Egress Hardware Group, ASSA ABLOY

"Big data and AI are coexisting together. The IoT is producing massive amounts of data and the pipe that's taking all that data is less expensive. **DATA DRIVES PRODUCTS**."

–Rob Martens, Futurist and VP, Strategy & Partnerships, Allegion.

"**CYBERSECURITY IS NOW A SHARED RESPONSIBILITY**. We need to know how a product can be used as a Trojan horse to break into the network and its information. This could take companies out of business very quickly. This is being discussed by customers today—more than the quality of video."

–Fredrik Nilsson, VP, Americas, AXIS Communications

"As a systems integrator **WE WANT TO MAKE SURE WE AREN'T DOING ANY HARM TO THE CUSTOMER'S NETWORK** and their systems aren't a vector for compromise. We have to make sure our customers are protected."

–Ken Lochiatto, President and CEO, Convergint Technologies

"Cybersecurity can be a great differentiator for the business. **WE ARE PUTTING A SKU LINE IN FOR CYBERSECURITY**."

–Herve Fages, VP, Connected Buildings, Honeywell

"Big data is life changing in how we operate buildings and determining our future role. It's all about how to pull that information out that benefits the customer. **BIG DATA CHANGES THE WAY IN WHICH WE SERVICE CUSTOMERS**."

–Lisa Roy, Vice President, Integration and Commercial Operations, Building Solutions-North America, Johnson Controls Inc.

"The ability of people to control a large portion of their life through **THE SMARTPHONE HAS BECOME TRANSFORMATIVE**."

–Michael O'Neal, President, Nortek Security & Controls

"**WHO'S GOING TO BE MY UBER**? Who's going to come in and reinvent the space?"

–Tim Williams, Vice Chairman, Pinkerton Global Security Services

"With increasing connectivity comes additional threat vectors from which adversaries come at us. There's deep interplay between cyber and physical worlds. Now cybersecurity is an indispensable and inextricable aspect of advancing the industry. **WE ARE NO LONGER GUNS, GATES, GUARDS AND GEEKS, BUT A 'DO ALL, BY ALL.'"**

–John McClurg, Vice President, Office of Security and Trust, Cylance

"**EVERYBODY WANTS RMR, BUT CONSUMERS DON'T WANT TO SUBSCRIBE TO A LONG-TERM CONTRACT** if the services are the same from provider to provider. The onus is on us to create good service. It has to be backed by a tangible service for the customer to get it."

–Brian Lohse, Senior Director, Commercial Platforms, Alarm.com

"**THERE'S DIRECT CORRELATION BETWEEN THE LEVEL OF ENGAGEMENT AND ATTRITION.** We need to help consumers manage their life better."

–Jeffrey R. Gardner, CEO, MONI

"Disruption and innovation can come at you from a hundred different angles. **YOU HAVE TO DECIDE WHAT YOUR STRENGTHS AND YOUR CORE INNOVATION TO FOCUS ON**."

–Jay Darfler, SVP, Emerging Markets and Innovation, ADT Security Services

"**THERE'S AN AMAZING AMOUNT OF PRIVATE EQUITY CAPITAL IN THE MARKET**. When there is money to do deals, valuations go up. There's also significant uptick in the lower end of the market."

–John Mack, EVP, Co-Head, Investment Banking and Head, Mergers and Acquisitions, Imperial Capital

"**RING IS ANOTHER EXAMPLE OF TALENT OUTSIDE THE INDUSTRY COMING IN AND CREATING OPPORTUNITY AND DISRUPTIVE CAPABILITIES**. We are seeing talent coming in from broader industries and helping us take the industry to the next level."

–Robert Chefitz, Managing Partner, Egis Capital Partners

INTRODUCTION

REFINING THE VISION

10 MEGATRENDS TRANSFORMING THE INDUSTRY

WHEN THE SECURITY INDUSTRY ASSOCIATION (SIA) introduced the 2017 inaugural Security Megatrends™ as a compilation of forward-thinking insights chronicling the transformation of the physical security industry, the publication predicted a rapidly morphing landscape. Fast forward to this year's Securing New Ground (SNG™) conference—and the developments have held true and escalated in quick-step fashion—perhaps faster than we envisioned.

Many trends identified have remained and evolved with technological advancements. But consistent among all those is a continued refinement of those movements. Not only has the industry become more sophisticated in physical security, information technology, logical security and cyber, but so have the outside forces redefining the vision of security. Now, the forces affecting security manufacturers and practitioners have further broadened–and physical security disciplines have become responsible for mining data and intelligence–contributing to an overall better business outcome and tangible return on investment for customers.

Some of the overriding trends reshaping the industry:

- The ongoing and continued proliferation of the Internet of Things (IoT) and connected devices
- Cybersecurity—new challenges and convergence with physical security
- Smart and Big Data—the impact of emerging artificial intelligence, augmented reality and machine learning
- Evolution of risk management to encompass physical and logical security in proactive and predictive risk management analysis
- Continued transformation of the security installer and integrator channels into "everything as a service," with models embracing the cloud, interactive services, DIY and self-installation markets
- Entrance of entrepreneurial buyers and outsiders who find potential revenue streams attractive
- Mobile everything, cloud computing and emerging remote services
- Social media and its impact upon emergency communications
- Emerging connected services and a customer experience focusing not on product, but real value

"We are living in the most exciting times in the history of modern technology," said Steven Van Till, President and CEO of Brivo and Chairman of SIA Standards. "Technological currents have converged and amplified and remixed with each other to accelerate the pace of innovation. Now, physical security is no longer just physical—modern security systems are cyber-physical systems, inheriting both the power and pitfalls of the digital world."

SNG, presented by SIA, encapsulates the thought leadership in the transformation of physical security. SNG is a roadmap written by leading executives, security providers and manufacturers, with their view from the top of an industry seeing a converged entity of comprehensive risk management, physical security, safety and cybersecurity.

What are the most forward-thinking solutions we can provide our customers for security, safety, cyber control and convenience? Those are the marching orders moving into 2018 and beyond.

MEGATRENDS

BOOMING GROWTH OF THE INTERNET OF THINGS (IoT)

UNBRIDLED CONNECTIVITY MOVING TO NEW MARKETS

CONNECTED DEVICES, AKA IoT, continues to grow at an unprecedented rate and is redefining every consumer, business and market—especially security. Integration, convergence and connectivity with a growing array of sensors, systems and devices puts physical security on the cusp of new services, while standing guard to deter, detect and defend new compromises from open, interconnected solutions.

Gartner Inc., Stamford, Connecticut, forecasts 8.4 billion connected things deployed worldwide in 2017, up 31 percent from 2016 and projected to reach 20.4 billion by 2020. Total spending on endpoints and services was expected to reach almost $2 trillion in 2017. Businesses are on pace to employ 3.1 billion connected things in 2017 and just as the Bring Your Own Device (BYOD) brought concerns of the security of network-connected devices, those challenges will be even more extreme for corporations and industries leveraging IoT for business operations.

According to Gartner, worldwide spending will be in the trillions in just a few years and while consumer applications will make up the majority of connected devices, enterprise spending will still lag.

While there will be more consumer devices in the market, enterprise businesses are also likely to ramp up their use of connected solutions in the coming years. Businesses are predicted to represent more than half of overall IoT spending in 2017 at 57 percent.

Specific industry verticals, such as process sensors for electrical generating plants or real-time location devices in healthcare will predominantly drive this trend. But going into 2018, cross-industry devices like those used in smart buildings—such as LED lighting and physical security systems—will take the lead. By 2020, Gartner expects cross-industry devices to reach 4.4 billion units worldwide, with vertical industry-specific devices at 3.2 billion in use.

"THE IOT IS ACCELERATING IN MATURITY AND ADOPTION. THE CORE ELEMENTS OF MORE ACCESSIBLE AND LESS EXPENSIVE SENSORS, DATA TRANSPORT OPTIONS AND DATA ANALYSIS TOOLS ARE CONTRIBUTING TO THE MISSING ELEMENT FACILITY EXECUTIVES, PROPERTY MANAGERS, CIOS AND USERS HAVE BEEN LOOKING FOR: CONVENIENCE."

—ROB MARTENS, FUTURIST AND VICE PRESIDENT OF STRATEGY AND PARTNERSHIPS, ALLEGION

There will be 50 billion connected devices by 2020, according to Cisco and other industry reports. By 2018, it is predicted that 66 percent of networks will have an IoT security breach, according to IDC Research.

SENSING AS A SERVICE

Analysts from Forrester Research warn that as the IoT becomes more rapidly interconnected with the physical world, the consequences of security failure will escalate. As a result, the emphasis on client safety, industrial operations and national infrastructure will overshadow the protection of client data and become priorities. It's up to the security industry to determine how it should position itself and react—especially when the IoT is growing faster than our ability to secure it.

The IoT is proliferating new challenges and capabilities to the physical security and risk management sectors. The result, when implemented and secured properly, will be predictive analysis and complete situational awareness from top to bottom and the ability to deliver a more personalized experience to all users.

GARTNER TOP 10 STRATEGIC TECHNOLOGY TRENDS FOR 2018

Table 1: IoT Units Installed Base by Category (Millions of Units)

Category	2016	2017	2018	2020
Consumer	3,963.0	5,244.3	7,036.3	12,863.0
Business: Cross-Industry	1,102.1	1,501.0	2,132.6	4,381.4
Business: Vertical-Specific	1,316.6	1,635.4	2,027.7	3,171.0
Grand Total	**6,381.8**	**8,380.6**	**11,196.6**	**20,415.4**

Source: Gartner (January 2017)

CYBER MEETS PHYSICAL SECURITY

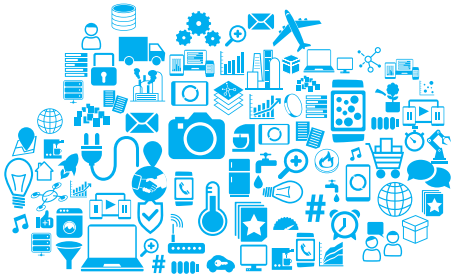
THREATS MAGNIFY WITH DIGITAL INNOVATION

CYBERTHREATS AND RANSOMWARE continue to present a major threat across all businesses and vertical markets. According to Trend Micro's annual security assessment report, 2016 Security Roundup: A Record Year for Enterprise Threats, cyberthreats climbed to an all-time high, with ransomware gaining popularity among cybercriminals looking to extort businesses.

Cyberthreats are comprehensive in nature. As more systems become network-connected, the threat factor escalates. In January 2017 in Washington, D.C., just prior to the presidential inauguration, hackers were able to take over 70 percent of the network video recorders run by the city, leaving them unable to record for days. Reportedly, engineers were able to go to each location and conduct a system wipe and re-install, rather than handing over the ransom. The event showed the potential catastrophic effect and lengthy remediation period of ransomware, but other threats to the connected environment are also of concern.

NEW WI-FI VULNERABILITIES

In October 2017, the U.S. Computer Emergency Readiness Team warned users to update their devices to protect against a newly discovered vulnerability that affects nearly every modern, protected Wi-Fi network. A security expert at the University of Leuven in Belgium published findings that showed a widely used encryption system for wireless networks could give attackers an opening to steal sensitive information such as emails, chat histories and credit card numbers. Any device that supports Wi-Fi could be vulnerable to this attack, called Key Reinstallation Attack or KRACK.



Internet of Things

- Household appliances
- Driverless cars
- Cameras
- Human organs (Brains)
- SCADA Systems
  - Monitors and controls critical processes

Increasing connectivity = more avenues of attack

The Equifax consumer credit reporting agency was hacked and information compromised and stolen. The hack affected an estimated 143 million customers and cybercriminals could gain access to customer's personal information such as names, birth dates, addresses, driver's license numbers and even Social Security credentials.

With the ongoing trend to greater integration between sensors and devices with the IoT and other automations, the physical security industry is on high alert.

According to the Federal Communication Commission's (FCC) Cybersecurity Risk Reduction White Paper, issued on Jan. 18, 2017, "reasonable network management must include practices to ensure network security and integrity, including by addressing traffic harmful to the network such as denial of service attacks. The white paper expressed concerns about the "burgeoning and insecure IoT market [that] exacerbates cybersecurity investment shortfalls [because] the private sector may not have sufficient incentives to invest in cybersecurity beyond their own corporate interests."

> **"THE MODEL BY WHICH WE COLLABORATE AND EXCHANGE INFORMATION HAS TO CHANGE IF THE PHYSICAL SECURITY INDUSTRY WANTS TO REMAIN RELEVANT AND MOVE FROM REACTIVE TO PROACTIVE PREVENTION AND PRE-ACTIVE EXECUTION."**
>
> —JOHN MCCLURG, VICE PRESIDENT IN THE OFFICE OF SECURITY AND TRUST, CYLANCE/FORMER CSO OF DELL

Now, as total convergence of systems solutions continues, manufacturers are charged with dealing with an increasingly hostile environment. Manufacturers and systems integrators need to take physical security systems to the next level, providing hardened solutions with additional cybersafeguards built in and offering the most up-to-date methods to protect network connected devices. Underwriters Laboratories (UL) recently launched a new Cybersecurity Assurance Program called UL CAP. It uses the UL 2900 series of standards to offer testable cybersecurity criteria for network-connectable products and systems to assess software vulnerabilities and weaknesses, minimize exploitation, address known malware, review security controls and increase security awareness.

Security integrators are now beginning to offer cybersecurity as a service, as they continue to grow their businesses from hardware-centric to solution-oriented models that meet the current and future needs of consumers and markets to address ongoing vulnerabilities. If customers are exposed—they will not be forgiving. They expect service providers to be their trusted advisors—companies they can count on for the latest protection and detection, whether security or cyberthreats.

ACCESSING AND ANALYZING SMART AND BIG DATA

MOVING INTO ARTIFICIAL INTELLIGENCE AND AUGMENTED REALITY

EVERY MINUTE, more than 400 hours of video are uploaded onto YouTube, 156 million e-mail messages sent and 3.8 million searches conducted on Google. By the year 2020, about 1.7 megabytes of new information will be created every second for every person.

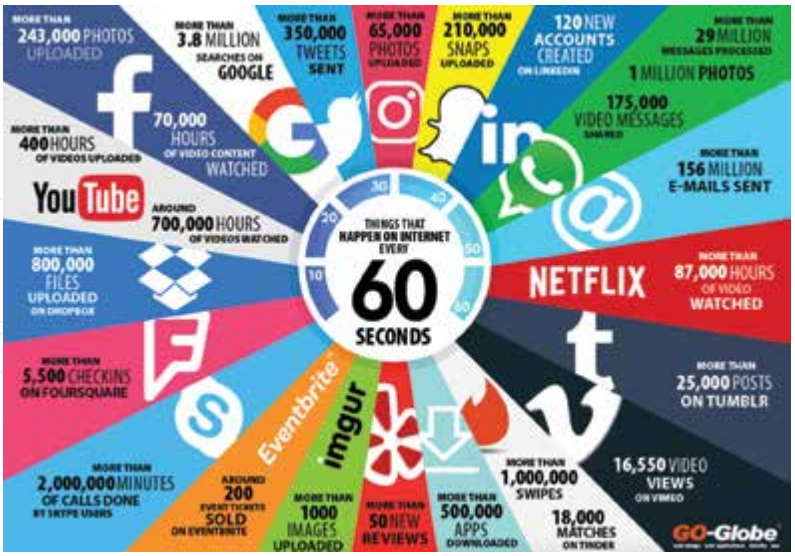
Those statistics only scratch the surface of data generation, which spans to sensors, medical records, corporate databases and more.

As we record and generate a growing amount of data every millisecond, we also need to be able to understand this data quickly. From monitoring traffic to tracking epidemic spreads to trading stocks, time is of the essence. A few seconds' delay in understanding information could cost not only business operations and process, but also lives.

Less than 0.5 percent of all data is ever analyzed and used. Yet it represents opportunities for added intelligence when properly segmented so it becomes smarter—and faster—leading to powerful, real-time insights.

DATA BRINGS HEIGHTENED PERFORMANCE

For a typical Fortune 1000 company, just a 10 percent increase in data accessibility will result in more than $65 million additional net income, according to Forbes.com. For the physical security industry, smart and big data represents challenges and opportunities in mining the right data, getting information quickly and putting it to use for greater safety, security, risk management and business intelligence. Data helps security providers personalize the customer experience and add value to their suite of services.



> **"DATA IS THE CURRENCY OF THE MODERN WORLD."**
>
> —LORNE TERRY, SALES DIRECTOR—CANADA, HIKVISION

Data is generated in several ways, with sensors being the most common form via the IoT. All this data is great, but how is it directed securely? Is it protected and segmented properly so it's smart and intuitive and provides additional critical information so the protected premises can be proactive rather than reactive? How do we provide the right cybercontrols so all this data isn't compromised? These are some of the questions—and challenges—as we continue to delve into new areas of information collection, consolidation and actionable data that assists manufacturers, security providers and end users.

Data needs to be smart or targeted so that it makes sense for businesses. It should be able to identify weaknesses in the protected premises and provide algorithms that allow for predictive analysis. It also needs to enable real-time decision making.

Because this time to acquire additional insights is increasingly important, it will incorporate video analytics, artificial intelligence and augmented reality (AR). AR is an emerging technology, but physical security experts are already anticipating how it will impact the industry. Unlike virtual reality, which completely immerses the user in a digital world, augmented reality keeps the user functional in the real world by superimposing digital information, such as images or GPS data, onto the user's real-world view. In the example of first responders, a firefighter may have AR built into their head gear, showing the structure of the mass notification system, emergency communications and even building and floor plans.

Security practitioners need to have a plan for the data they are collecting and a realistic risk assessment of the exposure of this data to their companies and clients.

MEGATREND 4

EVOLUTION OF RISK MANAGEMENT

RISK MANAGEMENT TRANSCENDS DEPARTMENT TITLES

THE RISKS HAVE CHANGED and no organization, large or small, is immune from physical security threats, terrorism, hackers, organized crime and insider compromise. Corporate security is morphing into new disciplines and even employing counter intelligence practices to proactively address and plan for attacks which are wide-ranging and can include loss of information, credit card fraud, workplace violence, worker's compensation fraud, embezzlement, loss of proprietary information or compliance control.

Risk management and planning has broadened and the most effective plans focus on a holistic approach and collaboration between all stakeholders—extending beyond the chief security officer, security executive, C-suite and chief information security officer to include human resources, information technology, other employee stakeholders as well as suppliers and service providers.

The biggest gripe of security directors? When security companies lead with technology instead of consulting with security practitioners to investigate their challenges and the best ways to mitigate potential risk and loss of business continuity or sensitive information.

"CONVERGENCE IS COMING INTO PLAY, ESPECIALLY FOR THOSE WHO CAN SUCCESSFULLY INTEGRATE CYBER AND PHYSICAL SECURITY. THE INTEGRATION OF ALL THESE DATA SOURCES WILL DEVELOP INTO 'HEADS UP' DASHBOARDS YOU CAN USE IN REAL TIME ON A CONVERGED PLATFORM TO GET ALL THE INFORMATION INTO ONE INTERFACE SO USERS CAN UNDERSTAND THE THREAT IN FOCUSED MANNER."

–TIM WILLIAMS, VICE CHAIRMAN, PINKERTON

COLLABORATION SETS THE STAGE

Nothing is 100 percent secure. Just as physical security relies on layers of detection and protection, so does cybersecurity. Risks, and their evaluation need to use new tools to assess, monitor and maximize mitigation. Other indicators can include social media, "dark web" criminal activity monitoring, real-time reporting of arrests and even proceedings from court findings. Silos of responsibility will no longer make the grade. A coordinated approach, input and accountability between a variety of functions in a company will bolster the cause. The most successful models include all corporate stakeholders and possible sources of information to circumvent loss and reduce the potential for insider risk threats.

The age of big and smart data and artificial intelligence will play a role in successful risk mitigation. Users need targeted data they can use in predictive analysis that will help identify threats before they become reality.

Security providers need to work closely with security directors and all stakeholders to take physical security systems to higher levels and provide the most trending safeguards possible. Today, security providers are the experts end users are turning to for advice and tactics to prevent cyberthreats, ransomware and other malicious attacks on physical security systems which may circumvent the network or provide access to customer data.

TRANSFORMATION OF THE CHANNEL

SERVICE MODEL REDEFINES THE BUSINESS

WHAT'S A TYPICAL SECURITY PROVIDER LOOK LIKE TODAY? The answer could be anybody's guess, because now, there are more players than ever, coming from all points of the business and various vertical markets and competencies.

There's an ongoing, heightened transformation of the security installer and integrator business into everything as a service, with new models embracing interactive products, DIY and self-installation markets. Outsiders from the IT sectors or start-ups have entered the business and traditional security monitoring companies are now offering DIY or self-install systems.

This year alone, Ring launched Protect, a $199 connected home security system; Best Buy and partner Vivint expanded their smart home retail offering; Honeywell announced a DIY solution; ASSA ABLOY acquired August Home; Nest Labs introduced a DIY home security solution, Nest Secure, with MONI Smart Security providing professional monitoring service for the systems.

"CLEARLY THERE IS A PARADIGM SHIFT HAPPENING WHERE HISTORICALLY THE CORE OF OPERATIONS WAS MONITORING SERVICE AND EVERYTHING ELSE WAS PRODUCT CENTRIC. NOW, WITH ADVANCEMENTS OF CLOUD SERVICES WE ARE SEEING THAT CHANGE."

—BRIAN LOHSE, SENIOR DIRECTOR, COMMERCIAL PLATFORMS, ALARM.COM

CONTRACTS CHANGING OR DISAPPEARING

Research firm IHS Markit expects that the "flexibility of month-to-month contracts from professional providers and DIY purchases/installation combined with no contract monitoring will begin to challenge the traditional model of paying for two-year, three-year or even five-year contracts."

With so many developments occurring rapidly, the traditional security provider should continue to change—and focus on value-added services that heighten the customer experience while delivering convenience and intelligence expected by every consumer. Focusing on value, price becomes less of a concern to customers. In addition, the new role of service providers also includes an assurance that the systems they deliver will be cybersecured—and as such security dealers will be looking for those manufacturers and technology partners with cyber-hardened network-connected products.

From the end user's perspective, security executives are looking for security providers who can collaborate fully to address current and future risks, leveraging analytics and data to assist not only with security and safety, but contribute to business continuity and promote a tangible return on investment.

The days of installing widgets are over—services will reign. Monitoring revenues will be tied to shorter, month-to-month contracts versus traditional long-term agreements that previously spanned years. The key to success is differentiation. Successful companies will differentiate themselves with indispensable services to the customer and solutions that make it easier for a consumer or company to be smarter, safer and less reactive.

SHAKE UP OF THE STATUS QUO

ENTRANCE OF ENTREPRENEURIAL BUYERS AND OUTSIDERS

NEW MODELS. NEW PEOPLE. NEW IDEAS. The pie is getting smaller, but each piece is more substantial. Strategic acquirers are snapping up and merging with traditional security manufacturers and installation companies. There's a bevy of new entrants, startups and IT-prolific companies entering the attractive security market. They bring refined ways of doing business and new efficiencies focusing on data analytics, convergence and IoT.

The industry's active investors, lenders and deal makers have kept busy with the active physical security landscape and the rise of new technologies—adding value to both the installation and manufacturing entities in the sector.

According to IHS Markit, security startup companies are becoming more commonplace in the industry. A variety of multi-system operators (MSOs), including Comcast, AT&T and Cox Communications shook up the U.S. intrusion market from 2013 to 2015. According to the research company's consumer video surveillance studies in 2015 companies that were two years old or less accounted for six percent of global consumer video-camera market revenues. By 2016, this had grown to over nine percent.

"WE ARE SEEING THE ENTRANCE OF A NEW CLASS OF ENTREPRENEUR COMING INTO THE INDUSTRY RAISING LARGE AMOUNTS OF CAPITAL."

—ROBERT CHEFITZ, MANAGING PARTNER, EGIS CAPITAL PARTNERS

WHY IS THIS HAPPENING?

The industry's largest players are growing as new technologies and applications reach residential and even transcend traditional small-to-medium business markets. But there are challenges and the recurring revenue model is changing from hardware and project based to income from service, maintenance and increasingly, remote monitoring from cloud and interactive services.

Service creates value, but monetary values are changing. The industry's long-time recurring monthly revenue (RMR) centric model is over 25 years old and much of the capital used to achieve this high level of RMR has provided attractive returns for security alarm companies, one of the principal reasons private equity finds such keen interest in security. Today, 60 percent of the top 25 alarm companies in the security industry are backed by private equity investors.

Because the industry is changing from monitoring-centric revenue, the variables that have been in place for decades are being challenged. Subscriber acquisition costs (SAC) have increased and RMR margins have dropped. In addition, technology obsolesce has escalated, with service providers and manufacturing facing shorter product development cycles associated with more frequent technological innovation.

No contracts? It's becoming the norm and will ultimately influence company valuation.

Interoperability is also becoming a key consumer concern. Consumers are now more wary of purchasing products that will not be able to integrate with their existing security/smart home devices. Non-proprietary and open systems selected by installation companies will defuse these concerns.

MOBILE EVERYTHING

CONVENIENCE AND CONSTANT CONNECTIVITY REIGN

WHAT'S THE ONE ITEM MOST PEOPLE WON'T LEAVE HOME WITHOUT? Their smartphone.

Mobile technology is becoming synonymous with access identity and credentialing and many consumers are now comfortable using their devices to access their home or office and check in on the residence or facility with connected video in addition to pay for products or services on the go.

According to new research from the Consumer Technology Association (CTA) U.S. Consumer Technology Sales and Forecasts, sales of connected devices are projected to reach 635 million units in 2017—a record high total and six percent year-over-year increase from 2016. Smartphone unit volume grew three percent to reach 185 million smartphones shipping in 2017, with revenues expected to reach $55.6 billion for a two percent increase.

Mobile technology is also incorporating more physical security features. Earlier this year, Apple announced its new smartphone, iPhone X. It doesn't include a 'Touch ID' fingerprint authentication system, but instead checks that your identity is authentic with 'Face ID' which is used to unlock the phone and authorize payments.

"IN FIVE TO 10 YEARS WE WILL BE USING OUR PHONES TO GET INTO WORK, PERHAPS SUPPLEMENTED WITH MECHANICAL DEVICES AND HARD CREDENTIALS. IT'S HARD TO IMAGE THAT WON'T HAPPEN AND THERE ARE LOTS OF IMPLICATIONS OF MANAGING THE CHANGE FROM A CARD TO DIGITAL IDENTITY."

—MARTIN HUDDART, PRESIDENT OF THE ACCESS AND EGRESS HARDWARE GROUP, ASSA ABLOY

Two recent reports from Gartner Inc. further predict a rapid migration to cloud-based physical access control systems (PACS) and mobile credentials.

The Predicts 2017 report from Gartner suggests that by 2020, 20 percent of organizations will use mobile credentials for physical access in place of traditional identification cards. A second report, Technology Insight for Physical Access Control, predicts that within a similar timeline, 20 percent of large organizations will use cloud-based PACS head ends to simplify deployment.

ONE DEVICE DOES IT ALL

For the security industry, the smartphone will be transformative within access control. Of course, this trend is tied to cloud computing and also perpetuates the move to open systems and away from proprietary access control. Replacing traditional physical access cards with smartphones enables both cost reductions and end user benefits as does the deployment of cloud-based PACS.

IHS Analyst Jimmy Dearing said that increased use of mobile credentials and new biometric technologies are the top hardware trends, along with logical/physical integrations and remote services. Mobile credential downloads were expected to rise from 4.5 million downloads in 2016 to 13.5 million this year.

By itself, mobile credentials in access control is a strong value proposition. But mobile credentials are also able to provide an integrated and higher value system for the user while it promotes new services and revenue streams.

CONTROL THROUGH CLOUD COMPUTING

DRIVING GREATER EFFICIENCIES AND PROMOTING MANAGED SERVICES

THE GLOBAL CLOUD COMPUTE SERVICES MARKET is expected to grow from $23.3 billion in 2016 to reach $68.4 billion in 2020 and 90 percent of organizations will adopt hybrid infrastructure management capabilities, market research firm Gartner predicted.

Growing connectivity and convergence and integration with IoT, mobile technology and a wide range of applications and services is driving cloud hosting and the use of public, private and hybrid clouds. Users are now comfortable with the cloud, using it for many years for online banking, virtual conferencing and other tasks and services. Many companies today are no longer brick and mortar, operating primarily from a cloud-hosted infrastructure. Airbnb Inc., Uber and many others continue their success in leveraging the cloud for operations, circumventing a traditional business model.

Cloud computing, Software-as-a-Service (SaaS) and managed services continue to populate the physical security industry. As security providers transition more fully into networked connected devices and information technology (IT), embracing the cloud hosting will be paramount. Why? Because of the inherent efficiencies, safeguards, scalability and accessibility of this virtual physical security management system solution.

GREATER CONTROL WITH THE CLOUD

For solution providers, there's opportunity in providing managed services and subsequent RMR that is highly attainable with the cloud—remote testing and maintenance, system resets, scheduling, management of credentials and more—anywhere there is an internet connection. These and other services provide nascent opportunity for security providers to add new revenue streams with hosted systems. With the cloud and its "always on, always accessible" platform, systems integrators can become total solution providers and the indispensable contractor customers count on for all their system installations.

> **"CLOUD TO CLOUD INTEGRATIONS USING WEB SERVICES MAKE THE NEED FOR GLOBAL STANDARDS BETWEEN ECOSYSTEMS LESS IMPORTANT, ALLOWING MORE COMPETITION. THERE MAY NEVER BE A STANDARDS OR PLATFORM WINNER."**
>
> —FREDRIK NILSSON, VICE PRESIDENT, AMERICAS, AXIS COMMUNICATIONS

When it comes to the emerging field of cybersecurity, the cloud puts service providers in the right place, with inherent data security safeguards such as two-factor authentication, encryption and SSL certifications. Cloud-hosted solutions also include automatic backup, disaster recovery and updates so the user is always working off the latest secured platform.

There's another bright spot in the cloud-hosting scenario. Although legacy equipment isn't the safest access control environment, cloud hosted access control can actually help this equation by integrating with most existing equipment, fostering use of the secure cloud environment. Cloud-hosted access control systems are often hardware agnostic and can be configured for communication with many legacy devices on site, so the user isn't forced into a total replacement. In addition, the use of cloud hosting sets up the user to deploy a variety of multi-technology devices and peripherals, so providers can add devices and expand their portfolio of managed service offerings.

The cloud is an enabling technology. It enables the user greater access to managing their premises. It also enables savvy providers to offer new services, remotely access and manage systems for a top notch user experience. All this leads to greater confidence in the service provider and a more satisfied customer who is less likely to discontinue the services that have become so valuable to their home or business.

CLOUD COMPUTING DEPLOYMENT MODELS

Private

A cloud computing model in which an enterprise uses a proprietary architecture and runs cloud servers within its own data center

CHARACTERISTICS:

Single-tenant architecture

On-premises hardware

Direct control of underlying cloud infrastructure

TOP VENDORS:

HPE, VMware, Dell EMC, IBM, Red Hat, Microsoft, OpenStack

Hybrid

A cloud computing model that includes a mix of on-premises, private cloud and third-party public cloud services with orchestration between the two platforms

CHARACTERISTICS:

Cloud bursting capabilities

Benefits of both public and private environments

TOP VENDORS:

A combination of both public and private cloud providers

Public

A cloud computing model in which a third-party provider makes compute resources available to the general public over the internet. With public cloud, enterprises do not have to set up and maintain their own cloud servers in house

CHARACTERISTICS:

Multi-tenant architecture

Pay-as-you-go pricing model

TOP VENDORS:

AWS, Microsoft Azure, Google Cloud Platform

INTEGRATING WITH SOCIAL MEDIA

DISRUPTIVE AND DRIVING FORCE

SOCIAL MEDIA—including Twitter, Facebook, Instagram, SnapChat, LinkedIn and others—continue to drive communications. For the physical security industry, it also has become an enabler for promoting business and connecting with customers, especially millennial and younger buying demographics who are "always connected." In law enforcement and emergency communications and operations, social media has become critical in identifying active shooters, criminal activities or other potential threats or disasters in real time.

Geo-location services inherent in social media are critical for first responders who know the IP address of the person initiating the communication and can pinpoint their location quickly and accurately. Sharing information on this platform can mitigate risk and allow law enforcement to better identify and neutralize attackers before they have an opportunity to cause harm. Police departments regularly search Facebook and Twitter to locate criminal suspects or get tips on their whereabouts.

Social media continues to foster situational awareness and promote proactive emergency management. Some of it is self-enforced. In an interesting twist, a Facebook user said he would turn himself into police after committing a crime when he got 1,000 "likes," which happened after only days.

EMERGENCY COMMUNICATIONS TOOL

Facebook, now with 2 billion monthly active users, is transforming disaster response with its Safety Check Tool, a personalized breaking news service which allows users to confirm their whereabouts and let others know they are safe and out of harm's way. It was used extensively during the Pulse night club shooting in June 2016 in Orlando. Referred to as a crisis hub, it's a live, centralized repository for information and media about any given disaster, where people can not only check on the safety of individuals but also coordinate ways of responding in the physical world, follow news and chatter and even monitor live video coming in from scenes.

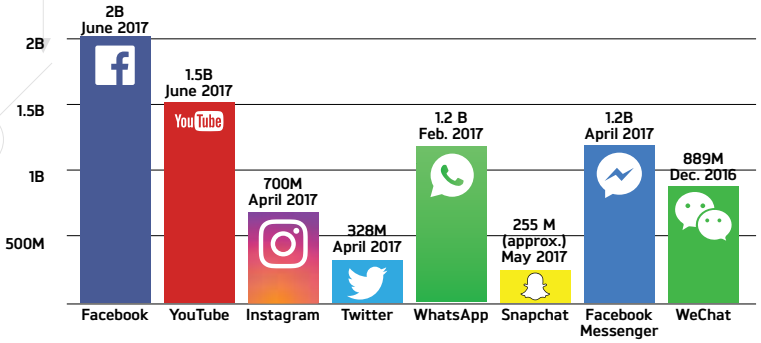
"IN 2012 WE EXPERIENCED A RIOT AT MALL OF AMERICA THAT STARTED THROUGH SOCIAL MEDIA. FOLLOWING, WE DEVELOPED A SOCIAL MEDIA AWARENESS PLATFORM AND STAFFED UP FOR MONITORING THIS ACTIVITY, INCORPORATING TRADITIONAL DISPATCH, SOCIAL MEDIA AND MONITORING AND EMERGENCY OPERATIONS CENTERS. THOSE ARE THE ASSETS YOU NEED TO RESPOND IN CRISIS."

—DOUG REYNOLDS, DIRECTOR OF SECURITY, MALL OF AMERICA

The next step for social media is deeper integration with mass notification and emergency communications—with the ability to disseminate specification information to individuals who may need to be evacuated or take shelter in place. The most effective scenario would combine social media with technology. For example, video surveillance and analytics detect a vehicle traveling in the wrong direction in a public area or bridge and send an automatic alert directly to social media platforms in real time.

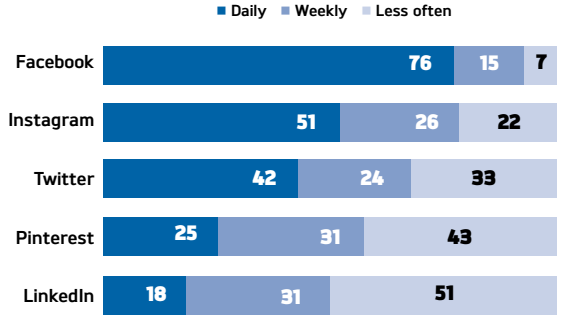
Social media can be a force multiplier to improve response and provide proactive insights. As the IoT and other disciplines continue to merge and converge, social media will be part of the integration of critical information resources.

SOCIAL MEDIA MONTHLY USERS



Source: Techcrunch.com

SOCIAL MEDIA USAGE



Source: Pew Research Center, March 7 –April 4, 2016

EMERGING CONNECTED SERVICES

CONSUMERS WANT CONVENIENCE AT THEIR FINGERTIPS

THE SECURITY INDUSTRY DATES TO THE FIRST BURGLAR ALARM produced by Edwin Holmes in 1857. For much of its longevity, security has struggled to reach double digits in saturation in the home market.

Welcome to 2017. Now, security has taken its place as a holistic experience equated with connectivity, convenience and integration with other systems that enhance the lifestyle of consumers and provide a solid return on investment for business users. The experience starts with a security system control, but now also ties in video, smart sensors, energy management, water detection and automating devices.

The models for security have changed and vary dramatically. There are traditional companies supporting DIY or self-install markets. New entrants are diving in hoping to get a piece of the growing market. It's extremely disruptive times for security providers who don't change and adopt a new way of business, or by contrast, quite attractive for those who are responsive, nimble and looking ahead to the future.

Technology is changing—rapidly. A new generation of smart home sensors, which ABI Research predicts in its report: "The Future of Sensors in the Smart Home," will approach 4.5 billion installations globally by 2022 is destined to fundamentally alter how homes are built, maintained and managed.

Sensors embedded in a wide range of smart home devices and appliances will deliver near real-time analytics on changes within home environments. The ability to transform this data into valuable systems and services will be at the heart of smart home adoption and the future housing market, according to ABI Research. Voice control, artificial intelligence and analytics are other far-reaching technologies poised to change how security is perceived and sold.

The ongoing IoT, convergence and integration will assist in the proliferation of security. Products like Amazon Alexa and Google Home most likely will soon integrate with traditional security systems.

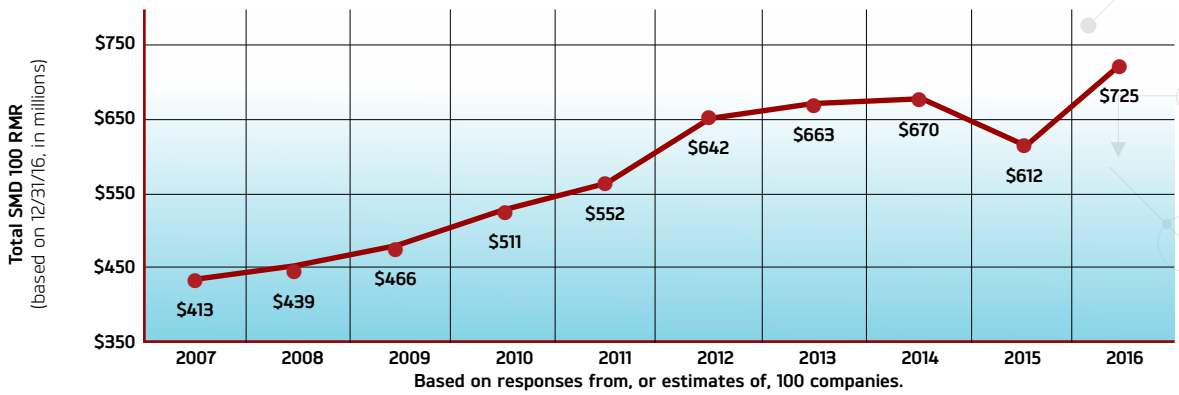
EASY IS THE ONLY WAY

Customers want seamless connectivity. They want to quickly and automatically get updates and never want to have to refer to a manual. Has anyone ever reviewed the operating manual for an iPhone? They don't want to know what the equipment is—they want to know how it can help them save energy, automate daily functions, or allow for remote access and other conveniences.

The cloud is also part of a progressive service provider's conversation. It provides seamless access to systems and allows for offering upgrades and other services. The cloud also enables security companies to provide service and maintenance remotely—so companies can avoid costly site visits, lowering labor costs and controlling the customer experience from any connected device quickly.

It's a changing landscape and security providers will now be able to provide a value proposition to the commercial market that will be able to lower their business costs, such as energy management and lighting control. Security providers who can adapt, provide services and help the customer increase profitability will also be able to increase their value and positioning in the competitive landscape.

RMR: UP 18.4 PERCENT TO $725 MILLION



Source: 2017 SDM 100, SDM Magazine, May 2017

securityindustry.org
8405 Colesville Rd.,
Suite 500
Silver Spring, MD 20910
301-804-4700