2019 SECURITY MEGATRENDS™

THE ANNUAL VISION FOR THE SECURITY INDUSTRY

SIA
SECURITY INDUSTRY ASSOCIATION

STAFF

SCOTT SCHAFER
SIA Chairman of the Board
scottschafer@securityindustry.org

DON ERICKSON
SIA CEO
derickson@securityindustry.org

GEOFF KOHL
SIA Director of Marketing
gkohl@securityindustry.org

KARA KLEIN
SIA Communications Manager
kklein@securityindustry.org

JOSEPH GITTENS
SIA Director of Standards
jgittens@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 Contributing 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
securityindustry.org

2019 SECURITY
MEGATRENDS™

EMBRACE CHANGE

Physical security moves into its most formative years

THE SECURITY INDUSTRY IS AT A PIVOTAL POINT IN ITS DEVELOPMENT. It's about embracing change—adapting to meet the new needs of the consuming public in as safe and convenient a method as possible. It's about disruptive technology—and how it can be used for a competitive advantage in the digital age. It's about developing new strategies and thought processes.

If any particular group is the most cognizant of changes in technology, it's probably the physical security industry. Systems are increasingly open, and more devices and sensors are connected. With this openness come cyber risk and data privacy concerns. Ten years ago, cybersecurity was rarely discussed among practitioners; now, it's one of the first questions on a client or prospect's mind as they ask, "What are you doing to protect my company and customer data and physical security information? What safeguards are you using on the network, and are products vetted for cyber resiliency?"

Appropriately enough, our top Security Megatrend for 2019 is cybersecurity's impact on the physical security industry, and it's having an effect up and down the landscape, from security implementations to hiring skilled talent.

Many other areas of the industry are in fluctuation, too. The entrance of global consumer electronics companies continues, now to the likes of Google, Amazon and Apple; do-it-yourself (DIY) systems are becoming more prevalent in residential, monitoring revenues are eroding and professional services need to adjust their go-to-market strategies as hardware margins are reduced.

The digital transformation permeates every aspect and vertical market—bringing new challenges that range from harvesting and delivering big data to customers to the identity management of the future. The industry continues to look strong from an investment standpoint, but changes are afoot as exit transactions for private equity investments of three to five years are on the pipeline.

"We continue to experience a bull market for 10 years now," said John Mack III, executive vice president, co-head of investment banking and head of mergers and acquisitions at Imperial Capital. "We are seeing more volatility coming into the back end of the market, but even so, we are in a pretty good space from a Wall Street perspective, with valuation at or near all-time highs and very active public and private capital markets."

These are the realities of the security industry and the vision into 2019 and beyond.

Sincerely,
Scott Schafer
Chairman, SIA Board of Directors

HOW WE PRODUCED THE 2019 SECURITY MEGATRENDS

Each year at Securing New Ground (SNG), senior-level industry leaders and financial partners gather, trends are discussed, connections are formed and minds are opened. SNG is about what people are thinking and what's going to shape them in the future.

In advance of SNG, we surveyed hundreds of executives from SIA member companies, along with current and recent speakers and attendees of SNG. We sought to identify which previous trends were still relevant, which trends were no longer as impactful to the industry and which broad trends needed to be added to our report.

In addition to the Security Megatrends, in our research we saw emphasis on other trends that, while not "mega," were nonetheless impacting the industry. Using the research data, we identified the most prominent of these "microtrends" and capture them on page 26 of this year's report. For the first time this year, we also encouraged respondents to identify areas within our industry that are poised for disruption, and those are recognized herein (p. 27).

In addition to the survey research, the selection of these trends relies on the speakers, panel and audience members of SNG, because the conference is the ultimate breeding ground for deep-dive discussions on what we can do as an industry to pave a successful future.

SNG is the ultimate business intelligence platform—designed to give you real information you can apply to your business or take to the community to forge our efforts, whether in cybersecurity, alarm verification, cloud computing or competing with the giants.

Through our 2018 research and the vetting, validation and additional research that occurs during and after SNG, here we have, hopefully, not only captured the industry's driving forces in the 2019 SIA Security Megatrends report, but also provided you insights and action items to facilitate a successful future in the security industry.

THANK YOU

SIA THANKS ITS 2018 SNG SPONSORS

ASSA ABLOY

SIEMENS

HID®

LENEL·S2 United Technologies

ANIXTER

Arecont Vision® A COSTAR COMPANY

AXIS® COMMUNICATIONS

BOSCH

Convergint® TECHNOLOGIES Making a Daily Difference

CapitalSource

alhua TECHNOLOGY

ISS

LOUROE ELECTRONICS World Leader in Audio Monitoring Technology Since 1979

milestone

NORTEK™ SECURITY & CONTROL

G4S

Genetec™

GSRMA

Hanwha Techwin America

HIKVISION®

Imperial Capital®

Panasonic

PSA® SECURITY NETWORK

RAYMOND JAMES®

SECURICON

INDUSTRY PARTNER

ISC INTERNATIONAL SECURITY CONFERENCE & EXPOSITION

MEDIA PARTNERS

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

SDM New Directions for Security Systems & Integration

SECURITY SALES & INTEGRATION

SECURITY SOLUTIONS FOR ENABLING AND ASSURING BUSINESS

EXECUTIVE TAKEAWAYS

OVERHEARD AT SECURING NEW GROUND 2018

SNG™
SECURING NEW GROUND®

"Cybersecurity is a topic that's at the forefront of everyone's mind because the impact is so significant. From readers and credentials to printers and coders, you're only as strong as your weakest link."

– Jeff Stanek, president and general manager, LenelS2

"It's not just about applying the latest patches anymore. This is a big opportunity to make sure your solutions address cybersecurity threats."

– Stefan Widing, executive vice president and head of global technologies, HID Global

"We need to encourage companies to share ideas that can help you grow and mature the company. Get the creativity pool going; tap young minds to join the security industry; get the right people in the right roles to maximize their potential and productivity. As an organization, we've changed to be less of a true hierarchy and more of a flat matrix where everyone in management is accessible and rolls up their sleeves. This encourage employee participation and make them feel part of a bigger team."

– Jody Ross, vice president of global sales and business development, AMAG Technology

"The Internet of Things (IoT), cloud, analytics, big data, artificial intelligence (AI), cybersecurity, mobile—those are all important facets of the solution, and that's a pretty interesting industry. This is an industry people would probably flock to, but they don't know enough about it."

– Scott Schafer, chairman, SIA Board of Directors

"A significant disruptor is the move to DIY. The business model changes are significant. Not only will DIY impact the balance of the security business, but it has the potential to impact the commercial space."

– Mike O'Neal, president, Nortek Security & Control

"It's official, there is a transformative change in structure taking place in GSA contracting for 2019 to modernize the GSA Schedule Contract program."

– Lynn de Seve, president, GSA Schedules Inc.

"It's great to have all these devices, but we're creating more problems than we have answers for long term. We need to build in a way to control these devices."

– Westley McDuffie, chief security analyst, IBM

"Police and fire are both skeptical of technology. We've wrestled with AI, and it was introduced too early, so we face a historical bias. Now we've partnered with companies to have learning labs to understand more about the technology before introducing it."

– Jack Hanagriff, law enforcement liaison, City of Houston

"None of us set out to be women in the industry; we set out to be the best people in the industry."

– Sandy Jones, founder and principal, Sandra Jones & Co.

"We approach our business with relationships. We are the eyes and ears of our customers, and we have seen the change. It is more about finding the solution for the customer and building flexibility for the future. That benefits both us and our customer."

– Eva Mach, president and CEO, Pro-Tec Design

"We need to be having conversations among different users and organizations rather than just within the security industry. We need to look for other security stakeholders we can work with. Having them at the table at the beginning is absolutely critical."

– David McGowan, vice president, global protection services, Tiffany & Co.

"AI will be disruptive in our industry. It will help us develop products; it may also help the bad guys infiltrate the security industry."

– Kim Loy, director of technology and communications, Vanderbilt Industries

"The ability to operate in an open environment is imperative today. If you aren't open or don't have a plan to be, I have no room for you in my enterprise."

– John Petruzzi, vice president, integrated security solutions, G4S Americas

“It’s no surprise that if we want to see our technologies grow, it has to be a community that wants to work together for a greater cause and purpose. We also have to consider ourselves as enablers. How are we allowing other people to innovate on top of what we do? When the community comes together, technology accelerates.”

– Mike Sherwood, director, technical operations, Milestone Systems

“Interoperability between business management and security systems is a crucial driver to the security industry as it moves to cloud computing and storage.”

– Stephanie Mayes, vice president of business development, Synectics

“If it doesn’t integrate, it’s very unlikely that we will invest in that platform.”

– Jerome Pickett, senior vice president and CSO, National Basketball Association

“Security and surveillance technologies have progressed tremendously over recent years with emphasis on the cloud, enterprise-level integrations and artificial intelligence. These trending topics are surely being driven by new levels of system intelligence, but the reality is that we as an industry are not quite there yet."

– Janet Fenner, chief marketing officer, ISS

“The number-one touch point for our customers is video; some 80 percent indicated an interest in cameras.”

– Doug Bassett, senior director, licensing and field compliance, Xfinity Home

“Video surveillance has become the largest generator of new data in the world by far, necessitating evolution of underlying video infrastructure solutions. But the security industry is generally very slow to adopt modern IT solutions, which opens the door to an accelerated influx of large, mature IT solution and service providers.”

– 2018 SIA Security Megatrends survey respondent

2019 SECURITY **MEGATRENDS**

MEGATREND 1

CYBERSECURITY IMPACT ON PHYSICAL SECURITY

CONTINUAL PROCESS IMPROVEMENT AND INVESTMENT NEEDED

IT'S HERE, IT'S NOW AND IT'S ACCELERATING. New cybersecurity risks emerge daily, morphing with new threats. It's the current landscape in which we live and will continue to test the physical security industry as we move to increasingly open environments, systems and connected devices propelled by IoT. It's about your business, your customer's business and vendors you do business with.

Cybersecurity is not a one-and-done deal; it's a constant examination of possible threats and risk to your organization and everything your organization touches. At stake are potential loss of business continuity, internal and customer data, proprietary company information and the reputation of the business.

Cyber threats are big business—where information and access are extremely valuable. These attacks range from amateurs to fully-funded nation state teams with the sole purpose of obtaining access to their target organization or industry. Once they infiltrate they gain information to attack physical access control systems (PACS) or other enterprise components. Cyber protection is more than firewalls, patches and passwords.

PERSPECTIVE

Valerie Thomas, executive consultant at Securicon, said the physical security industry needs to "lift the veil and take the mystery out of cybersecurity" during her SNG keynote address, Securing the Future of Physical Security. "Your industry is being targeted quite often and by people you don't understand. They are exploiting the technology you create to get closer to your customers' data."

NEW THREATS

Now that the industry is emerging from its silo, new threats present themselves. According to The Cybersecurity Imperative, published by ESI ThoughtLab and WSJ Pro Cybersecurity in partnership with SIA and a number of other organizations, "the rise of new technologies, such as artificial intelligence, the Internet of Things and blockchain, and the use of open platforms are seen as having the greatest impact on cyber risk."

STATS

While firms now report the biggest impacts from malware (81%), phishing (64%) and ransomware (63%), in two years, they expect massive growth in attacks through partners, customers and vendors (+247%), supply chains (+146%), denial of service (+144%), apps (+85%) and embedded systems (84%). Source: The Cybersecurity Imperative, a report from ESI ThoughtLab and WSJ Pro Cybersecurity

CHALLENGE

Digital innovation is a double-edged sword. While it improves business processes and outcomes, it also exposes companies to greater cyber threats presented by new technologies.

HOW THE COSTS OF CYBERATTACKS BREAK DOWN

Direct financial costs	56%
Fines and legal costs	55%
Productivity loss	46%
Intellectual property costs	40%
Replacement costs	38%
Response costs	36%
Reputational costs	30%
Opportunity costs	30%

POPULAR RECOMMENDATIONS

Common prescriptive advice related to cybersecurity of physical security solutions and systems includes the following:

- Eliminate default passwords in equipment and software
- Test and retest products internally and by an outside organization
- Establish a vulnerability tracking and reporting program
- Know your hardware's software and firmware
- Create a security resource center for your integrators and customers
- Update your internal security awareness training program
- Include cybersecurity in the product development process
- Remember that an effective cyber program is an ongoing process.

MEGATREND MOVEMENT

Cybersecurity replaced the IoT as the top Megatrend for 2019. In 2018, cybersecurity was ranked at 2, indicative of growing concern over loss of data, privacy and new attack vectors and actors at every level of the physical security business and from open, connected digital environments such as network-connected cameras and Wi-Fi.

TAKEAWAYS

Cybersecurity implementations are not a 'one and done' deal and require an ongoing examination of possible threats and proactive remedies.

Default passwords are still why most of the bad stuff happens.

Effectively managing cyber risk means service providers, manufacturers and customers have to continually invest and improve their cybersecurity postures as new risk profiles develop.

Privacy consultants and cybersecurity talent are a must-have investment for firms seeking resiliency.

MEGATREND 2

INTERNET OF THINGS AND THE BIG DATA EFFECT

MORE INFORMATION FROM EVERYTHING CONNECTED

THE SECURITY INDUSTRY IS AN EXCITING, ATTRACTIVE AND TECHNOLOGY-DRIVEN INDUSTRY delving into IoT, cloud, big data, analytics, AI, cybersecurity, drones, robotics, software as a service (SaaS) and more. There's data coming from everywhere. Now, the challenge is how to manage and segment all this information so it's usable and pertinent to the user.

PERSPECTIVES

" Today, modern physical security solutions are comprised of IoT devices and sensors that generate high volumes of security data. Applying analytics and AI systems makes this data more actionable and increases responsiveness for security systems users."

– SIA Chairman of the Board Scott Schafer

" There are certain key steps that should be taken early to enable data analytics, certain types of dashboarding, IoT enablement, etc. There is a responsible roadmap that should be created and understood, and we need to start taking steps toward that."

– Steve Schattmaier, director, data enabled business, Johnson Controls

" As we think about IoT, it's not about devices—it's about how you apply them. We have to think about a platform and a data strategy with three core tenants: identity, data and security. Those are the three core building blocks."

– Mike Foynes, Center of Innovation lead, Microsoft Global Real Estate and Security

CHALLENGES

- More data necessitates better ways to funnel and manage that data and get it to the user and even responding authorities in a cohesive manner.
- The IoT and other smart technologies will continue to disrupt the security of cyber-physical systems—which connects this trend back to the top Security Megatrend for 2019, cybersecurity. There's no line between the two—both need to be considered as the industry grapples with growing threats to connected security devices and all the data traversing open connections.

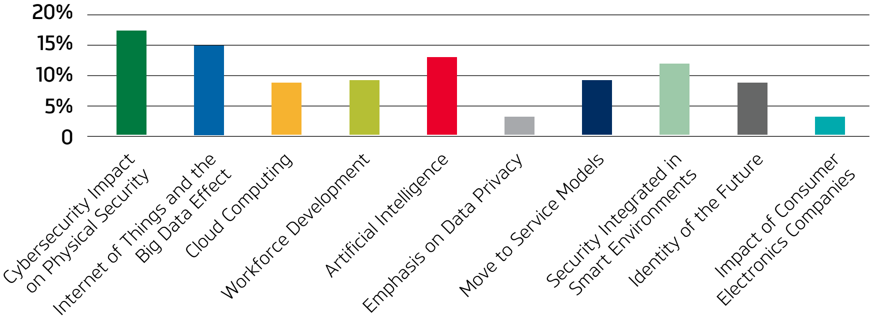
STATS

According to Statista, the installed base of IoT-connected devices and things is forecasted to reach a figure between 6.6 billion and 30 billion by 2020. Today, almost any physical object can be transformed into an IoT device if connected and controlled by the internet.

DISRUPTION

IoT and big data are related, along with their impact on the security industry, and it's more than just device connectivity. Big data could mean success—or failure—for companies that do not work to change and make use of all the information coming in. According to an Accenture study, 79 percent of enterprise executives agree that companies that do not embrace big data will lose their competitive positions and could face extinction. Even more, 83 percent, have pursued big data projects to seize a competitive edge.

WHAT IS THE SECURITY MEGATREND WITH THE BIGGEST POTENTIAL IMPACT ON SECURITY PRACTITIONERS?



TYPES OF BIG DATA ANALYTICS

	Descriptive	Diagnostic	Predictive	Prescriptive
Answers the question…	What happened?	Why did it happen?	What will happen next?	What should I do?
Level of advancement	Low	Medium	High	Very high
Incorporates AI and machine learning?	Not usually	Sometimes	Usually	Always
Level of popularity	Used by almost all organizations	Used by many organizations	Used by a smaller but growing group of organizations	Not yet widespread

Source: Datamation

MEGATREND MOVEMENT

A recurring Megatrend, the IoT moved from the top position to number 2 in 2019's Megatrends, obscured only slightly by the growing concern over cyber risk and threat. Big data, combined with smart data, was the third-ranked trend in 2018, moving up in 2019.

TAKEAWAYS

The physical security industry has an opportunity to build end-to-end solutions in a collaborative manner.

The conversation needs to shift from hardware to smart, available environments that benefit the end user with more than security and delve into business process improvement and market intelligence.

Data needs to be targeted, usable and correlated to the end user's needs.

MEGATREND 3

CLOUD COMPUTING

CLOUD GROWS—AND SO DO SECURITY AND TRANSPARENCY CONCERNS

CLOUD COMPUTING PLATFORMS AND APPLICATIONS ARE PROLIFERATING across enterprises today, serving as the IT infrastructure driving new digital businesses. The cloud is an enabling technology for security integrators, who can provide managed services and the cost and labor advantages of off-site servers to their customers.

PERSPECTIVES

To paraphrase SNG speaker Sal Mani: There's a need to leverage edge computing and integration with the cloud, in a hybrid approach, coupled with premier co-located servers.

> Why is cloud adoption so slow? We understand the efficiencies, but it's the interoperability, and we need assurances those cloud areas are actually, truly secure."
>
> *—Sal Mani, security systems program manager—Bay Area, Google*

> Everyone thought the cloud would be more secure, and it wasn't. That reality and some of the data have kind of made some chief information officers a little gun shy of new things."
>
> *—Harry Regan, vice president, Securicon*

STATS

According to IHS Market, the global off-premises cloud service market is forecasted to reach $414 billion in 2022.

CLOUD MODELS

Cloud computing, SaaS and managed services continue to populate the physical security industry. As security providers transition more fully into networked connected devices and IT, embracing cloud hosting will be critical to growth. There are inherent efficiencies, safeguards, scalability and accessibility benefits to this virtual physical security management system solution, especially for PACS.

PREDICTION

Cloud computing and edge computing will evolve as complementary models with cloud services managed not only on centralized servers, but also in distributed servers on premises and on increasingly reliable and stable edge devices.

CHALLENGES

How secure is the cloud? Does it offer interoperability and integration with other systems, services and processes? How can important video data be segmented to the cloud, without using massive amounts of storage? Now, edge computing is gaining acceptance and may be disrupting the traditional space.

WORLDWIDE PUBLIC CLOUD SERVICE REVENUE FORECAST

(Billions of U.S. Dollars)

	2017	2018	2019	2020	2021
Cloud Business Process Services (BPaaS)	42.6	46.4	50.1	54.1	58.4
Cloud Application Infrastructure Services (PaaS)	11.9	15.0	18.6	22.7	27.3
Cloud Application Services (SaaS)	60.2	73.6	87.2	101.9	117.1
Cloud Management and Security Services	8.7	10.5	12.3	14.1	16.1
Cloud System Infrastructure Services (IaaS)	30.0	40.8	52.9	67.4	83.5
Total Market	**153.5**	**186.4**	**221.4**	**260.2**	**302.5**

ADOPTION PATHS

- Access control is most dominant in current practical application, and use of the cloud for video is emerging strong, especially in the residential market, where consumers access video clips. Video in commercial has challenges with bandwidth and storage considerations, but advancing compression algorithms are providing some relief. In commercial applications where scalability is a mandate, the cloud is desirable and also provides logical access control and the ability to manage doors, locks and other physical security components. For other technologies, such as fire alarm signaling, mass notification and emergency communications, guided by codes, the road to cloud adoption may be much slower.
- The residential and consumer markets, where convenience rules, seem less concerned about security and instead look for ease of operation of a wide range of services, where the cloud excels. In commercial, however, end users are still leery, so there's a proving ground that needs to be demonstrated.

MEGATREND MOVEMENT

In the 2018 Megatrends report, cloud computing ranked number 8, and for 2019 it jumped to the number-three spot. The convenience and easy ability to add services and manage them cost effectively propelled it to this higher spot. But how will it shake out in 2020 and beyond as cited concerns play out or intensify?

TAKEAWAYS

Is a reverse shift possible? Is cloud computing losing favor as a safe method of security management?

There's a lack of regulatory compliance standards, unacceptable by high-risk and government users, stifling growth.

Security users are now looking at the increased flexibility and new wave of beefed-up edge computing, which has increased greatly in performance.

The conversation has also shifted to privacy and permanently segmenting and removing some customers' data and how and if that will be possible.

MEGATREND 4

WORKFORCE DEVELOPMENT

FINDING TALENT CHALLENGES ALL

NEW TO THE SECURITY MEGATRENDS RANKING FOR 2019 are workforce development and finding skilled employees in nearly every facet of the security industry. With unemployment at historically low rates, the trend in the technology sector and particularly physical security has accelerated and is inhibiting overall expansion.

Now, in addition to finding technicians with IT and networking skills, security stakeholders need employees well versed in cybersecurity, AI development and even privacy consulting. The goal at hand is to educate more students at a younger age that the security industry is high tech and exciting, through apprentice programs, high school mentoring and other outreach.

PERSPECTIVES

I visit underserved universities and talk to students about the security industry to grow interest in the field, bring new workers, diversify the industry and even reach people at the high school level."

–Eddie Reynolds, president and CEO, iluminar

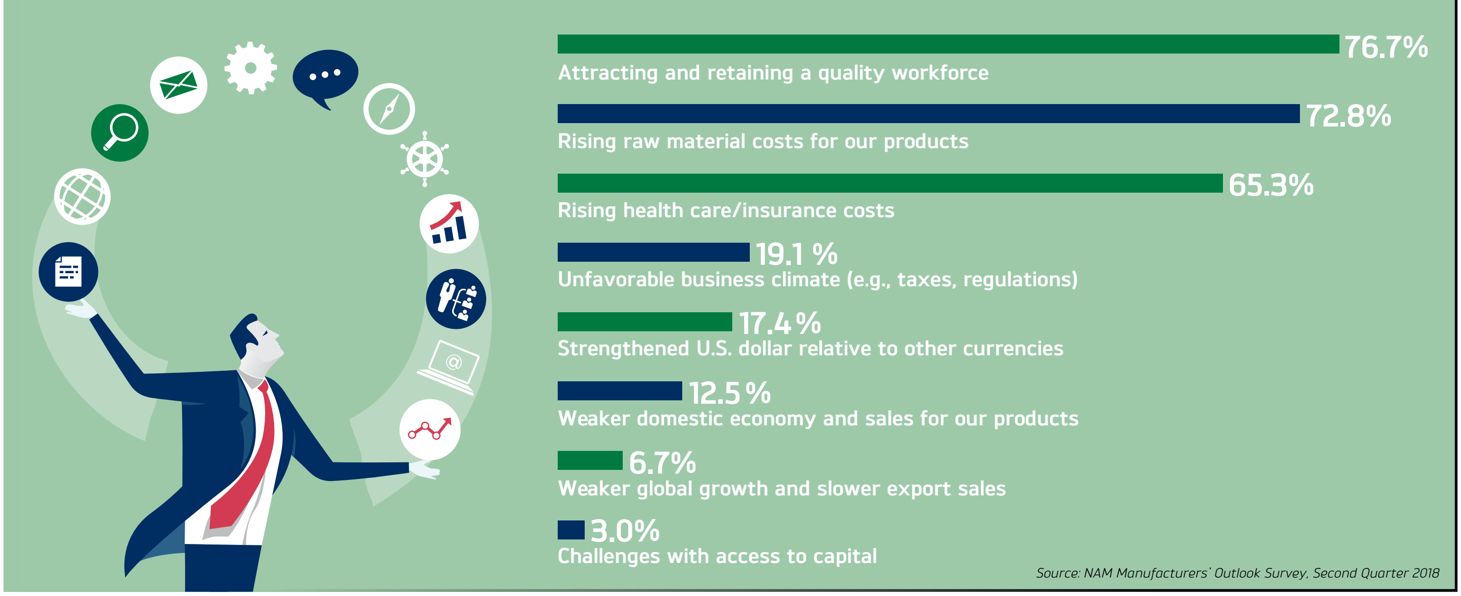
They can't find people, they can't afford them and it's the number-one problem. It's not just technicians or C-suite; the consensus is that it's everyone. This will have an impact and will be a huge impediment to growing the business."

– Bill Bozeman, president and CEO, PSA Security Network

We spend as much time as we can on in-house curriculum development, and we can't stay current–it's a huge challenge. There's no question the investment in training and education makes sense. Training and education really are standing in the way of rapid, more accelerated growth."

–Steve Firestone, president, Select Security

PRIMARY CURRENT BUSINESS CHALLENGES FOR MANUFACTURERS, Q2 2018



Source: NAM Manufacturers' Outlook Survey, Second Quarter 2018

STATS

The National Association of Manufacturers (NAM) says attracting and training a quality workforce is a top-cited challenge facing manufacturing firms. Source: NAM Manufacturers' Outlook Survey, Second Quarter 2018

CHALLENGES

- The physical security industry sits in the shadow of more visible, "sexy" technology industries, obscuring notable innovation that's occurred over the last several years. The industry is now high-tech, but it is still not recognized as such. The profile of the industry has to be positioned as progressive, innovative and IT-centric—attractive to job seekers.

- Attracting talent is a two-way street. New hires are no longer solely focused on wages and instead looking for work-life balance and career paths. Hiring companies are looking for enthusiasm and what potential employees bring to the table in cultural responsibility and creativity.

MEGATREND MOVEMENT

Workforce development is new to the 2019 Security Megatrends listing, showing the escalating problem of attracting new people to the industry and finding skilled talent.

TAKEAWAYS

AI is being leveraged in human resources screening processes, automated scheduling of interviews and keeping in touch with candidates during the hiring process.

The gig economy is alive and well, and companies may turn to this outsourcing lfor the long term or temporarily.

New research from McKinsey and Company notes that companies with more diverse workforces perform better financially.

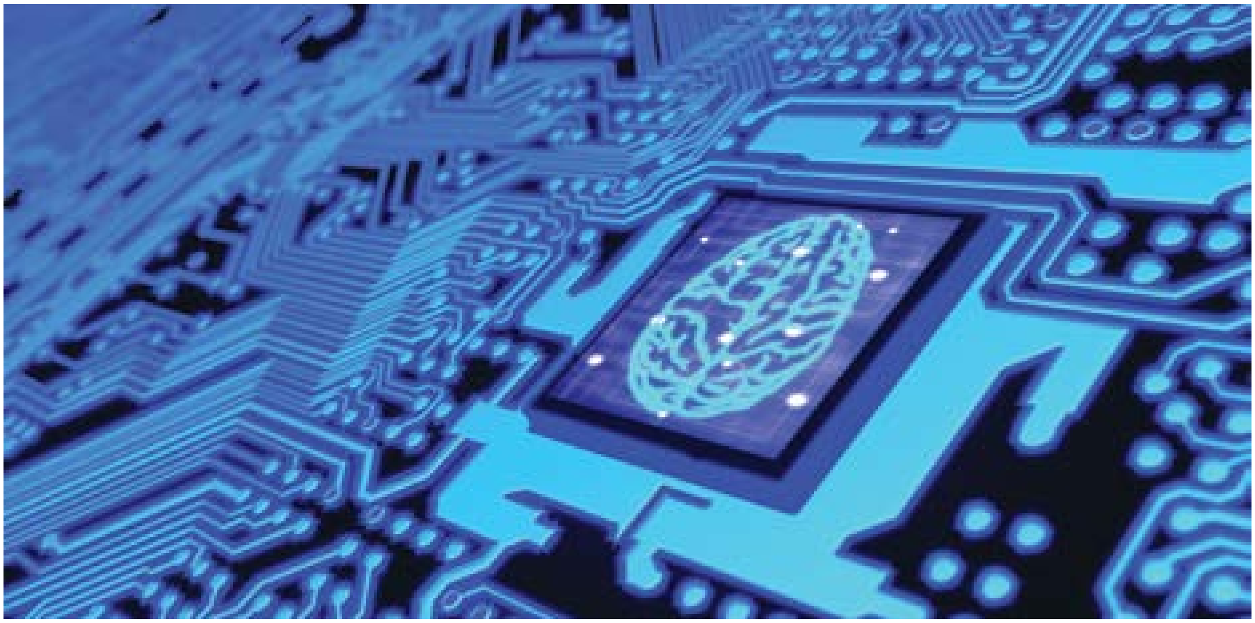
Engaging with local colleges and technical schools and providing subject matter experts to teach and lecture can provide ready access to talent.

Companies are focusing on entry-level positions and ramping up experience with in-house training.

MEGATREND 5

ARTIFICIAL INTELLIGENCE (AI)

MACHINE LEARNING IS THE FIRST STEP



GARTNER BELIEVES THAT 2018 WILL MARK THE BEGINNING of a "democratization of AI, extending its impact across a much broader swath of companies and governments than previously." The research firm further said AI will have a profound impact on how we will work—"some jobs will become obsolete, while others will be created and most will change. IT leaders must orchestrate changes in their enterprise's workforce as seriously as they seek to reap the business value of AI."

INFLUENCERS

According to McKinsey and Company, a convergence of algorithmic advances, data proliferation and tremendous increases in computing power and storage have propelled AI from hype to reality. AI is also being leveraged increasingly by startups and reducing barriers to entry in new markets.

HYPE OR SUBSTANCE

Like the video analytics push of several years ago, there's been some hype around AI, so some expectations have not been met. Most in the industry agree that AI applications need to be implemented and tested at the company level before widespread deployment.

PERSPECTIVE

" We leverage machine learning and AI to assess threats; where we want to go is enlightened AI where the technology has the morals to address specific issues."

–Nick Lovrien, chief global security officer, Facebook

CHALLENGE

Effectively deploying AI will take an investment by manufacturers, integrators and users, as well as education and training.

STATS

AI in the global, comprehensive security market is expected to grow exponentially in the coming years, according to a report by Market Research Engine. AI, specifically in the security segment, looks to exceed $35 billion by 2024.

ADOPTION PATH

AI/machine learning systems will advance the physical security industry and provide more value to end users, because these systems will eventually lead to automated processing of the big data being generated by our industry's millions of devices (see Megatrend 2: IoT and the Big Data Effect). AI will require greater adoption by robot and drone developers for those systems to achieve the promises envisioned as truly autonomous solutions.

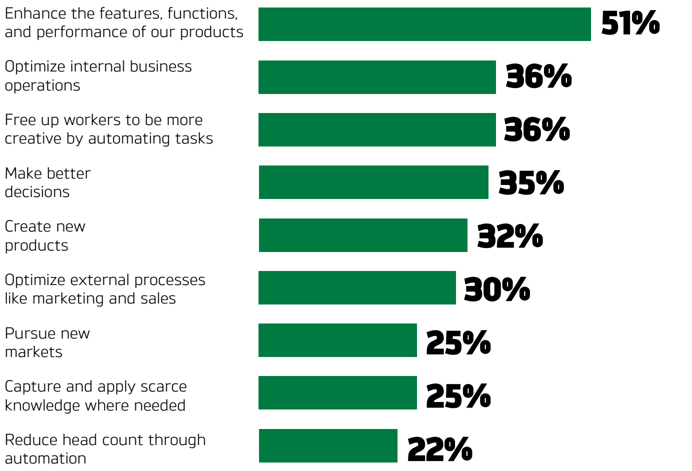
DISRUPTION

Using AI in business for targeted purposes delivers more flexible, insightful and increasingly autonomous systems, but AI won't necessarily reduce security jobs (at least in the near term); it will instead feed smarter information to professionals and responders.

THE BUSINESS BENEFITS OF AI

"We surveyed 250 executives who were familiar with their companies' use of cognitive technologies to learn about their goals for AI initiatives. More than half said their primary goal was to make existing products better. Reducing head count was mentioned by only 22%."

"Artificial Intelligence for the Real World" by Thomas H. Davenport and Rajeev Ronanki



Source: Deloitte 2017

PREDICTIONS

- AI in video applications is an obvious and immediate opportunity for security. In video, AI faces the challenge of generating so much data that can't be effectively reviewed without machine learning doing some of the groundwork. AI is also moving from commercial to residential applications, especially to verify activity before alarm initiation. Other areas which may emerge as strong players in AI applications for physical security include alarm monitoring verification, alarm arming and disarming (voice/smart speakers), predictive command centers, risk-based access control authentication, pulling data from other security or building management systems or social media alerts to make access decisions, security department operations, customer service and manufacturing.
- Video and video analytics will be used more extensively to create smart alarms for DIY and commercial security.

MEGATREND MOVEMENT

AI is another new Megatrend for 2019. As the technology has been refined, there have been more implementations and a proving ground for the technology.

TAKEAWAYS

AI will continue to advance and eventually augment portions of the security industry, like robotics and manned guarding.

Companies need to be their own test centers for AI before offering it to customers.

It all comes down to data, and whether AI information can be targeted specifically to assist with physical security risk, threat assessment and response.

MEGATREND 6

EMPHASIS ON DATA PRIVACY

CRIES FOR OPEN CONNECTIONS ELICIT NEW DATA CONCERNS

WITH A MOVEMENT TO CONNECTED SYSTEMS, cities, processes and people come new concerns over data privacy, also called information privacy. What's the ultimate balance between security and convenience, and what are people willing to give up to be able to have a seamless integrated solution? It's another dilemma the physical security industry must now address in the digital world.

PERSPECTIVES

"Digital technology is one of the key lenses through which we look at all our strategies. How do we identify, react and predict so we can manage and respond to risk more effectively? Digital worries me because of the risks it brings in. It's a tough environment, and we face it in a number of ways."

–David McGowan, vice president, global protection services, Tiffany & Co.

"Technology will be embedded in everything in the digital business of the future."

–David W. Cearley, vice president and Gartner fellow, Gartner Research & Advisory

CHALLENGES

- There's the issue of harnessing cyber-physical technologies effectively, as well as who is responsible for cybersecurity. For the end user, there's a need to better understand how safe the cloud is for their particular application. For the systems integrator, there's the opportunity to become an educational subject matter expert, building a relationship and educating the market on the digital transformation.

- "Data privacy at some point may become the most disruptive element facing any industry. As the world moves to a services- and data-oriented world, not only is cyber critical, but the 180-degree forces acting for preservation of data privacy are on a collision course of epic proportion." *(2018 SIA Security Megatrends survey respondent*)

ADOPTION PATH

Data privacy is directly connected to the IoT and the Big Data Effect megatrend. The number of connected devices in use worldwide now exceeds 17 billion, and the number of IoT devices is at 7 billion, according to research firm IoT Analytics. As we continue to add connected points, systems and services, the issue of privacy will accelerate.

*

GDPR: NOT OPTIONAL

The General Data Protection Regulation (GDPR), now governing the European Union (EU), is designed to unify data privacy laws. The directive focuses on keeping businesses more transparent and expanding the privacy rights of data subjects. When a serious data breach has been detected, the company is required by to notify all affected parties within 72 hours.

The rules encompass video surveillance data, cardholder information and activities tracked by an access control system, as well as license plate numbers captured by license plate recognition systems. Aspects of GDPR can also affect North America-based companies handling EU information and data processed within its borders and companies in noncompliance could face massive fines—four percent of a company's global earnings.

ANOTHER LAW TO WATCH

California recently passed the Connected Device Privacy Act, designed to ensure privacy and security of residents. The law requires manufacturers to provide connected devices with a "reasonable security feature or features" that are appropriate to their nature and function and ensure that the information they may collect, contain or transmit is guarded from "unauthorized access, destruction, use, modification or disclosure."

THE RIGHT TO BE FORGOTTEN

This concept and practice in both the EU and Argentina allows individuals to have information, photographs and videos deleted so they can't be found by internet search engine records. As privacy laws continue to emerge in the digital landscape, this trickle-down effect on video storage and archiving may present future challenges in surveillance, starting with whether recorded video can be permanently deleted. Maybe AI comes into play here as well, segmenting private data?

MEGATREND MOVEMENT

Entirely new for the 2019 Security Megatrends, data privacy didn't notch on the rankings for 2018. Now, with the GDPR and other privacy acts, open connections and interconnected systems, data privacy is an elevated concern.

TAKEAWAYS

Open systems require proactive data privacy processes.

Digital transformation is a necessity.

Users need strategies that will make them compliant across all their data collection processes as simply and cost effectively as possible.

MEGATREND 7

MOVE TO SERVICE MODELS

A FUNDAMENTAL BUSINESS SHIFT FOR SECURITY PROVIDERS

THE LATEST GENERATION OF HOME SECURITY TECHNOLOGIES is having a profound effect on installing companies in the industry. Hardware margins have shrunk, and DIY business models are holding strong. Amazon, Google, SimpliSafe and others with deep pockets for product development and marketing are raising the stakes—and the expectations of security end users.

Residential is all about ease of use and the customer experience. Customers want video, and cameras are often the lead-in to a connected home. Systems integrators are at an inflection point: they need to find a way to focus on services the customer wants and needs and move to a managed services model to make up for revenues now lost in equipment installation alone.

PERSPECTIVE

"There's an opportunity in technology to monitor new devices. The Best Buys and the Amazons will have an impact and at the same time create consumer awareness. If you are prepared, it could even bring you more opportunity."

–Christopher Baskin, CEO, American Two Way

"If you are in a market with these new technologies, we really think segmentation is critical. You need to understand who your customer is and the value proposition to them. Know your market and the nature of the market."

–Will Schmidt, managing director, security lending, CapitalSource

DISRUPTION

- Plug-and-play in the home is transcending into the commercial market, where users also want an easy and seamless experience. Even in the commercial space, particularly small commercial projects, it's time for the physical security installation model to adapt, because these trends will only intensify.
- The continued emergence of IT and audio/visual systems integrators in the physical security space will continue to apply pressure on security providers' business and service models.

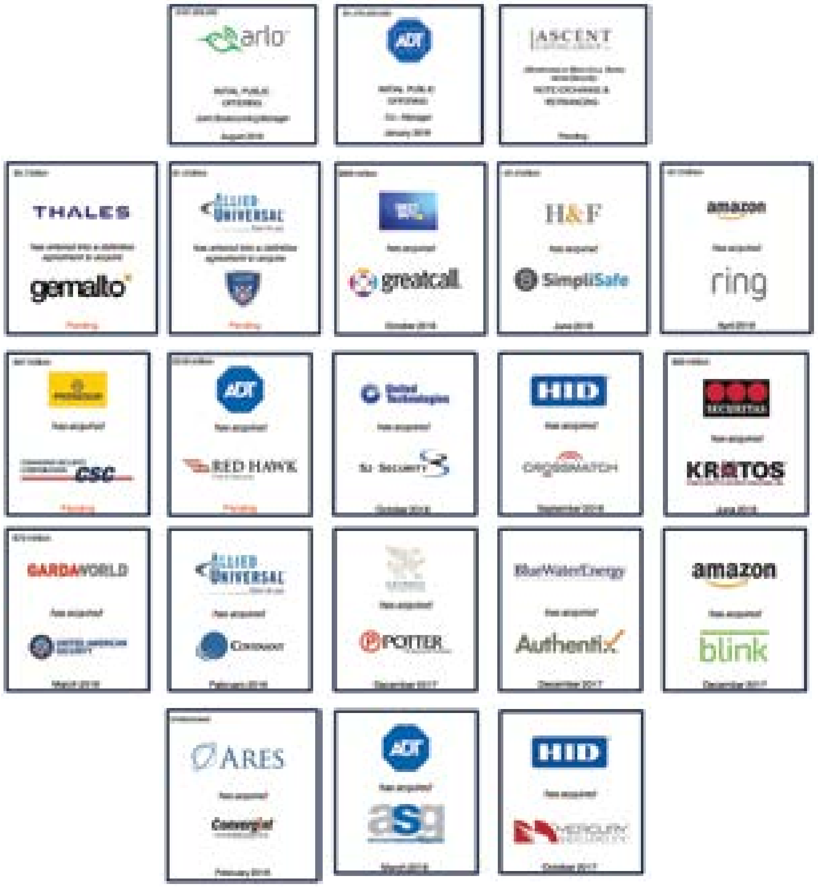
ADOPTION PATH

Is security moving to a DIY model? What's the right way for companies to succeed? Is it to offer new services and assist home owners with DIY in a hybrid approach, like Do It With Me? Other firms are decidedly emphasizing the value of professional installation, like ADT's new "Do It for You (DIfY)" residential campaign. The fact is, many homeowners who have DIY and non-monitored systems may move to monitored systems as they mature and start a family, so staying in touch and building relationships remains a necessity and market strategy.

CHALLENGES

Companies that are reluctant to shape their organizations into true services-first organizations may find that a sale of any device becomes an increasingly less attractive mix within the revenue portfolio.

SELECT TRANSACATIONS



MEGATREND MOVEMENT:

The move to service models dropped to number seven in the 2019 Megatrends. In 2018 it ranked number five (labeled the Transformation of the Channel), down a couple of notches and only obscured by more immediate issues.

TAKEAWAYS

Integrators need to take their managed service models to the next level by offering new services and devices.

In this volatile and changing installation environment, leasing systems may assist the smaller integrators in their changing business models. Manufacturers need to be convinced to help finance systems and help augment those new business models.

MEGATREND 8

SECURITY INTEGRATED IN SMART ENVIRONMENTS

THE NEXT WAVE OF CONNECTIVITY

EVERYTHING IS BECOMING CONNECTED—that's the IoT trend. And as new connected devices interface with each other, smart environments will begin to proliferate. Buildings may start with access control integrated with automation, HVAC or elevator control and expand to incorporate other areas. Security is hyper-connected, and the control panel often works with all systems—integrated on the hardware or software level. The pinnacle is the smart city, drawing in from all the different systems and services from connected buildings to make areas more responsive to its occupants and provide comprehensive safety and security. The "levels" of intelligence will rely on integration—and whether or not it's possible to achieve.

Smart cities are now conscious cities, pulling data, video and information from public and private entities. Systems are beginning to work on their own, learning with new data and becoming integrated and seamless. It's a challenge, an opportunity and a must in the future to make cities smarter, safer and more proactive.

PERSPECTIVE

> The brownfield on which cities are looking at can be lit up with a new suite of edge analytics. The emergence of a new class of edge analytics and deep learning provides new accuracy. Edge compute has vastly improved."
>
> *—Chris Bartos, vision team lead, Intel Corporation*

> Getting over the hurdle of testing and buying new technology is hard, but overall the smart city is about the integration of various sensor types and making meaningful relationships between all that data."
>
> *—Michael Joy, captain, Information Technology Bureau,*
> *New York City Police Department*

TOMORROW

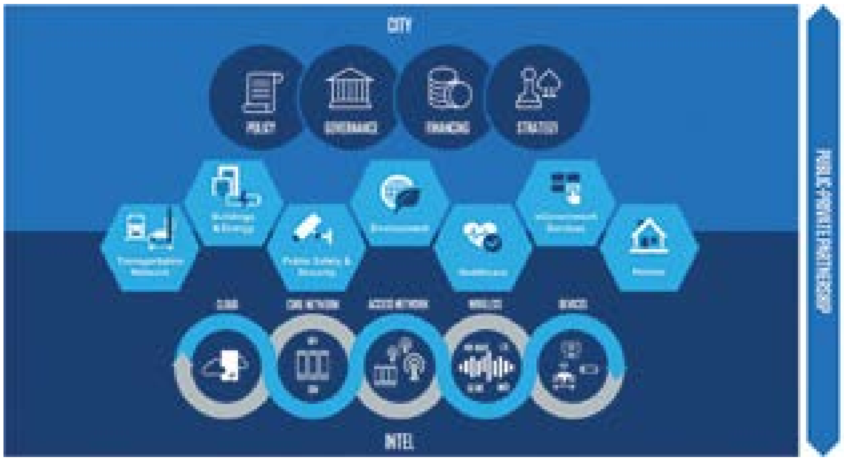
Smart cities will be more connected, networked and collaborative, according to Deloitte Insights, *Forces of Change: Smart Cities*. "Moving beyond just connected infrastructure and smarter things, the smart cities of tomorrow engage governments, citizens, visitors and businesses in an intelligent, connected ecosystem. The goal is to have better city services and a higher quality of life."

Installing sensors that collect data for optimizing the performance of physical devices is one part of what it takes to achieve the smart city, stated the report.

When connected sensors and systems come together in a cohesive, collaborative approach, smarter decisions can be made. Smart cities enable better decisions for all stakeholders. A truly smart city uses technology to promote better decision-making criteria for city officials and residents.

ADOPTION PATH

Analytics and AI will play a sizable role in the conscious city. Augmented analytics are also being discussed, as they focus on a specific area of augmented intelligence and leverage machine learning to determine how analytics content is developed, consumed and shared. Augmented analytics capabilities are expected to go mainstream for data preparation, data management, modern analytics, business process management, process mining and data science platforms. These insights from augmented analytics will also be prevalent in a variety of enterprise applications, including HR, finance, sales, marketing, customer service, procurement and asset management departments.



ELEMENTS OF A SMART CITY

Citizen Experiences & Services

A clear vision of the citizen services and experiences the city wants to provide

A Smart City Infrastructure

A foundation of technology-based solutions deeply integrated into every city operation, from strategic planning to service delivery, where agencies share data and collaborate in either real-time or regular cycles

An Enabling Environment

A coordinated strategy of key policies, good governance and sufficient financing to make the vision reality

Source: Intel

MEGATREND MOVEMENT:

New for 2019, the integration of security in smart environments (like smart cities) had not been recognized independently in either 2017 or 2018. However, this trend is closely related to the trends of IoT and Big Data, which have been ranked.

TAKEAWAYS

Smart is only as relevant as the data is to the end user.

Public-private partnership models will play an important role in smart city financing and funding.

5G wireless will be a big factor in infrastructure connectivity, offering more affordable connectivity.

End-to-end solutions need to be built, first bringing together manufacturers with end users in a collaborative approach.

MEGATREND 9

IDENTITY OF THE FUTURE

HOW WILL WE ENTER BUILDINGS TOMORROW?

FACIAL RECOGNITION IS GOING MAINSTREAM. Biometrics are increasingly reliable and cost effective, forging into new applications and markets. Speech recognition and sound are integrated increasingly into physical security, now in residential, with commercial on the horizon.

THE FUTURE

The identity of the future may be a single credential, or even a virtual certificate that identifies who you are and gives the system the ability to automatically revoke the permissions if protocols and compliances aren't followed. Whichever the case, the physical security industry needs to anticipate and adapt to ongoing technological changes in identity and visitor management.

PERSPECTIVE

"When I'm in my office, they don't trust me; everything is audited. It's zero trust, and that's hard to do in the normal security world. We have mapped how much longer it takes for authentication processes, and it's only about 15 seconds more for those safeguards."

– Sal Mani, security systems program manager–Bay Area, Google.

"The landscape of identity is changing, and tokenization schemes and the promise of a blockchain digital ledger will have an impact on federated yet unique identities."

–2018 SIA Security Megatrends survey respondent

CHALLENGES

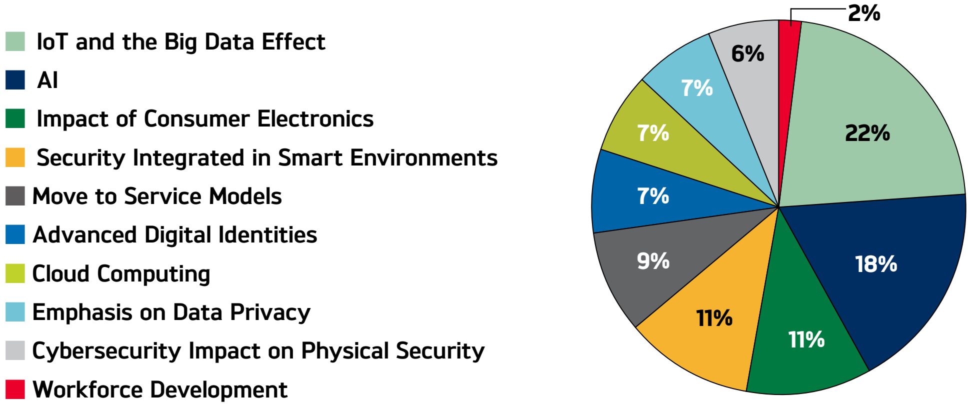
Consumers want convenience, but what about privacy? For residential users, seamless easy use outweighs most concerns over data compromise. In commercial, however, with regulations, compliance and standards often at bay, there's a need to balance ease of use yet still provide robust security.

As a Security Megatrends survey respondent noted, "Privacy issues may conflict with IoT and data search methods, which would impact proactive situational awareness and predictive analytics like facial recognition and data mining of social media."

FRICTION FREE

Frictionless access control, partly a buzzword and partly a vision for the future of access control, is the concept of free-flowing yet secure access to a space; it requires little interaction and does not interfere with users unnecessarily and eliminates the need for an employee to carry a token, such as a badge, or remember a PIN in order to gain entry into a building or office. Biometrics and radio frequency and technologies like Bluetooth can make this scenario possible. Frictionless means users are not slowed when accessing a building. Instead, their smartphones or other wireless credentials quickly allow access with little dwell time. The idea is convenience, but security needs to be balanced. The consuming public wants openness, but again, data and information privacy may be of concern.

WHICH OF THE 2019 SECURITY MEGATRENDS IS THE MOST UNDERRATED IN TERMS OF ITS POTENTIAL TO RESHAPE THE INDUSTRY?



MOBILE AS THE CREDENTIAL OF CHOICE

The smartphone has promise to become the carrier of the identity and access credential, as users are unlikely to leave it behind, making it a possible for frictionless and unified entrance control. It does, however, present other challenges, such as how to manage cybersecurity when the identity is on a user's personal hardware.

MEGATREND MOVEMENT:

Another newly identified Security Megatrend for 2019, the "Identity of the Future" trend has been spurred along by both technology advances and by consumers' increasing expectations of convenience and immediacy.

TAKEAWAYS

Security takes precedence, but factors are at play that dictate a smooth and seamless experience for the user.

A single digital identity that transcends logical and physical environments via sensor fusion (software that intelligently combines data from several sensors for the purpose of improving application or system performance) may emerge.

Improvements in facial recognition may finally push this long-running technology mainstream.

MEGATREND 10

IMPACT OF CONSUMER ELECTRONICS COMPANIES

THE RULES, AND PLAYERS, KEEP CHANGING

ONE OF THE MOST INFLUENCING FACTORS on the industry is the growth of consumer electronics companies and influx of DIY systems. Consumers are opting for video as a starting point for the connected home and usually not professional monitoring. Change in the physical security industry now continues at what seems like warp speed, influenced by increased consumer awareness and big buys such as Amazon's purchase of the Ring Protect system and its acquisition of Blink, a startup maker of wireless cameras. Statista research from 2018 puts the largest consumer electronics market in the world as the U.S., where market value of consumer electronics reached $107.1 billion in 2016. The strongest trend has been convergence, with the shift toward connected devices and telematics in the IoT another influencing factor in consumer electronics growth.

Firms like SimpliSafe are marketing security hardware directly to consumers, then adding services on top of the solutions. Speakers and sound seem to be the attractive entry points for both Google and Amazon with their smart speakers and voice control—but these systems are likely to become the gateways to the home. In the future, security systems may use these Alexa and Google Home systems as their primary interfaces with the customer.

DISRUPTION OR OPPORTUNITY?

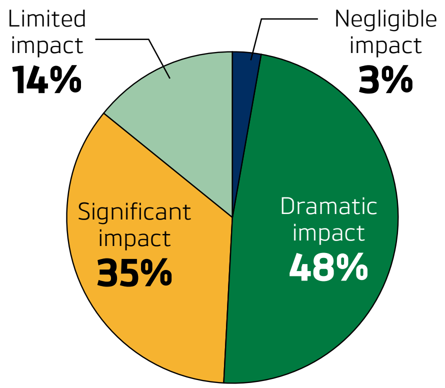
OPPORTUNITY: Recently, ADT announced a strategic initiative with Amazon to support integration of Amazon's new Alexa Guard feature with the ADT Pulse security system, leveraging sound detection via the customer's Echo device to listen for breaking glass and smoke or carbon monoxide alarms.

DISRUPTION OR OPPORTUNITY: Some see these bellwether changes as an opportunity to provide greater value to the subscriber or offer a new level of service. Others admit that it's a monumental sea change and that it will be difficult to keep pace and adapt effectively.

DISRUPTION POINT: Monitoring is also seeing substantial pressure. Most consumers are relying on smartphones as an interactive experience and to look in on their homes, watch their pets and children and provide remote care giver services. Professional monitoring may be an afterthought in residential, though the market for connected health services and personal emergency response due to grow with the aging population may help reverse that trend.

HOW MUCH OF AN IMPACT WILL THE CONSUMER TECHNOLOGY GIANTS HAVE ON THE INDUSTRY'S BOTTOM LINE IN THE RESIDENTIAL SPACE?

- 🟩 **Dramatic impact**
- 🟨 **Significant impact**
- 🟩 **Limited impact**
- 🟦 **Negligible impact**



Source: SNG 2018 audience poll

PERSPECTIVES

Most forecasters predict average recurring revenue will continue to drop significantly, but they remain optimistic about what this disruption brings.

> "There will be an opportunity to monitor new devices. The Best Buys and Amazons will have an impact and at the same time create consumer awareness, and for those who are prepared it could even bring more opportunity."
>
> *–Christopher Baskin, CEO, American Two Way*

> "This isn't a space anymore for small companies to dominate the industry. We have huge players with large infrastructures who have the ability to invest in technology and change the models. Comcast's Xfinity Home is a disruptor having a major impact on the smaller companies."
>
> *–Mike O'Neal, president, Nortek Security & Control*

MEGATREND MOVEMENT:

Technically a newly identified megatrend for 2019, this trend is intrinsically connected to 2018's Megatrend #10, connected services, and to 2018's Megatrend #6, "Shake-Up of the Status Quo."

TAKEAWAYS

Will physical security move fully to a Google/Amazon DIY model?

Will another model emerge along with new players?

Will traditional systems solution providers be able to carve a successful spot?

2019 SECURITY MICROTRENDS

SMALL BUT INFLUENTIAL FORCES AT PLAY

IN ADDITION TO THE SECURITY MEGATRENDS, there are many other influencing and disruptive factors at play in the broader physical security industry. As part of our annual industry survey, respondents identified what we're calling the Security Microtrends for 2019:

MICROTREND: POLITICAL ENVIRONMENT VOLATILITY

As one of our survey respondents noted, the political environment includes the following factors: tariffs, duties and issues of material and product "dumping," infrastructure security and intellectual property protection and espionage.

U.S. trade policy, particularly related to China, has been the most impactful aspect of this microtrend; it even impacted the 2018 National Defense Authorization Act in 2018, instituting a federal government purchasing restriction on the products of select Chinese firms.

As one survey respondent noted, "Changes in the political environment will start to have a growing impact on our businesses as we get hit with tariffs or security-based requirements. This extends to the requirements for the origin of products—that cameras can't come from China, etc."

MICROTREND: UNIFIED SYSTEM DELIVERY AND TECHNOLOGY ALLIANCES

Integrated open systems that provide meaningful data beyond security will help security providers differentiate themselves and add value. Technology alliances and open standards focusing on interoperability will be key to further industry development.

Proprietary technologies and siloed manufacturing are disappearing in favor of groups of companies working together in partnership to formulate a plug-and-play operative, a necessity if the industry is to compete with consumer electronics companies. Collaboration between vendors is peaking in an effort to further the industry.

> **"The political environment and tariffs are huge macrotrend that will have a very significant influence on our industry."**
>
> *– 2018 SIA Security Megatrends survey respondent*

> **"We're moving to total physical security in a bundle, with solutions arising from alliances created in the industry."**
>
> *– 2018 SIA Security Megatrends survey respondent*

> **"The Apple policy change to allow application developers to develop iOS apps that are not strictly involving Apple Pay will erupt a demand for near-field communication credentials and other security apps."**
>
> *– 2018 SIA Security Megatrends survey respondent*

MICROTREND: THE DREAM OF FRICTIONLESS ACCESS CONTROL

This microtrend connects with the overarching trend of the trend we're calling Identity of the Future (see page 22). But concerns remain: How secure is truly frictionless access control?

There's also the impact of mobile access control. Security users are becoming less reliant on separate credentials they must carry (e.g., key card, fob, PIN) and more able to use the things they want to use and are more convenient—phone, biometrics and even automated facial recognition.

MICROTREND: THE MOVEMENT TO SELF-MONITORING

Consumers are relying on their smartphones to watch their homes and even small businesses. But what does this mean in a real emergency? There's an opportunity for the physical security and monitoring industries to work together on the value proposition—and that centers on educating on the importance of professional central station services and response.

DISRUPTION POINTS FOR 2019

A LOOK AT THE AREAS OF THE INDUSTRY most likely to face challenges due to the Security Megatrends and Security Microtrends. We have identified three key disruption points:

1 DISRUPTION POINT: RESIDENTIAL AND MONITORING.

Residential is impacting commercial security, and commercial products are coming to the residential market. The lines are blurring with convenience, interconnectivity and simple operation key to users. Users are looking for a positive experience and the ability to control functionality from their phones. DIY systems will continue to infiltrate the landscape, but systems integrators can offer support services for those models or offer these systems themselves. Monitoring is also seeing a total transformation. Smartphones and video dominate for residential monitoring. New models may include monitoring on demand or other hybrid approaches that play off the growing DIY market, like Do-It-With-Me concepts.

Public Safety Answering Points (PSAPs) are being inundated with false alarms. Funding is scarce, and budgets are thin, for continued investment and growth. The movement is to NG911, which will enhance emergency number services by creating a faster, more resilient system that allows digital information (e.g., voice, photos, videos, text messages) to flow from the public through the 911 network and, eventually, directly to first responders. How can we get PSAPs to be part of the conversation and equation?

2 DISRUPTION POINT: DISTRIBUTION

Distribution is also seeing new models, with direct-to-consumer sites and new options for acquiring product beyond traditional channels. Traditional security products increasingly can be found from online retailers which were available previously through distribution only. Customers can now research and even purchase products on Amazon and other online channels, further affecting profitability margins and go-to-market strategies.

3 DISRUPTION POINT: MANNED GUARDING

Manned guarding, depending on who you ask, could either benefit from or be negatively impacted by technology forces at play; it could be bolstered by video analytics and AI, giving guards more complete information and allowing them to step into more data-empowered roles. This may also make guarding a more attractive, high-tech position. But there's the potential of robots entering the space, which may counter some of the more mundane tasks such as guard tours and also help relieve some of the shortages in staffing, but it could also ultimately lead to replacement of jobs by automated processes and robotics. Real-world deployment of robots will be the ultimate testing ground before the latter could occur.

“‘Good enough’ monitoring may eventually destroy the existing monitoring revenue/profit model. Today's central stations will need to: 1) do more with less, 2) find a way to continue to drive significant value in the eyes of customers who are heading toward being connected to everything all the time and 3) find a cost model that allows them to grow in an ever-increasing trend toward lower monitoring costs over time. There are simply too many companies that want to play in the sand box, and the big ones will not let go.”

– 2018 SIA Security Megatrends survey respondent

“Our business is becoming commoditized with price being dominant across product, service and connections. This will create new business models that could be disruptive. Nearly everyone is looking over their shoulder at Amazon, Google and Apple. They are not only competing for customers but have also been acquiring companies, driving up values for those companies and making it hard for us to compete.”

– SIA September 2018 survey respondent

SIA
SECURITY INDUSTRY ASSOCIATION

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