2020 SECURITY MEGATRENDS™

THE ANNUAL VISION FOR THE SECURITY INDUSTRY

SIA
SECURITY INDUSTRY ASSOCIATION

2020 SECURITY
MEGATRENDS™

STAFF

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

DON ERICKSON
SIA CEO
derickson@securityindustry.org

STEVE VAN TILL
Megatrends Advisor

GEOFF KOHL
SIA Senior 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 Member Services
kmurphy@securityindustry.org

MARC BENSON
Associate Director of Membership
mbenson@securityindustry.org

DEBORAH O'MARA
DLO Communications
Contributing Author

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

SECURITY INDUSTRY ASSOCIATION

SNG™
SECURING NEW GROUND

EVEN MORE RELEVANT

Tech advances. Business changes. Consumer concerns. The security industry's trends grow more complicated.

IN TODAY'S WORLD—ON BOTH COMMERCIAL AND RESIDENTIAL FRONTS—our industry's systems connect with more data sets and influence more systems than ever before. Our industry's solutions are tied into human resources and marketing systems, logical access systems that interconnect physical and network access, cybersecurity solutions, mechanical and comfort systems and even business operations and home automation systems.

It is truly a dynamic time to be in the security industry because these advances make our businesses more important and relevant to our customers—while calling us to think through and solve new challenges.

At the October 2019 Securing New Ground conference, the theme of the event's signature View From the Top panel session was "From Relays to Cyber and AI," and the discussion presented by this panel of leaders covered technology changes in addition to new ethical issues and privacy concerns created by technology advances. That range of topics really tells the story of the 2020 Security Megatrends you will find in this report.

When the Security Megatrends report was first produced (the 2017 edition), the focus on trends within the industry was heavily driven by tech advances and the proliferation of Internet of Things devices. Today, those technology trends are still in play, but what is evidenced in the 2020 Security Megatrends report is a much keener interest in privacy rights, how we protect our customers' data and how we navigate ethical, political and regulatory concerns.

In short, Security Megatrends is no longer a pure business and technology trends report, but a report that balances those trends with the concerns of consumers and the general public.

This shift in how we report the Security Megatrends speaks to the changing nature of the security industry. What may have once been may have been an industry of relatively straightforward and siloed devices—cameras that simply recorded to DVRs, readers and panels that simply opened a door, and infrared sensors that simply detected motion—is no longer an isolated industry.

Today our industry is connected—and not just device to device or even device to the network. It's increasingly connected to other industries, to the global economy, to global politics and to consumer trends and preferences. Our industry is influencing how businesses can be more efficient. Our industry is making consumers' lives safer and more convenient. Our industry is feeling change, and it is driving change. We hope this report helps you navigate those changes.

Sincerely,
Scott Schafer
Chairman, SIA Board of Directors

THANK YOU

SIA THANKS ITS 2019 SNG SPONSORS

ASSA ABLOY

HID

Johnson Controls

ALARM.COM

ALERT ENTERPRISE

ALLEGION

AXIS COMMUNICATIONS

BOSCH

Genetec

Hanwha Techwin America

LENEL·S2 United Technologies

HIKVISION

milestone

RAYMOND JAMES

ACRE

ARCULES

brivo simply better security

Convergint TECHNOLOGIES Making a Daily Difference

dormakaba

GSRMA

Imperial Capital

PACIFIC WESTERN BANK

PSA SECURITY NETWORK

MEDIA PARTNERS

SECURITY BUSINESS

SECURITY SALES & INTEGRATION

SDM

SECURITY SYSTEMS NEWS

INDUSTRY PARTNER

ISC INTERNATIONAL SECURITY CONFERENCE & EXPO

EXECUTIVE TAKEAWAYS

OVERHEARD AT SECURING NEW GROUND 2019

SNG™
SECURING NEW GROUND®

"We have the opportunity to move beyond just providing products and devices to experiences. We're asking consumers, 'What matters most to you? What's your mission—what are you trying to protect?', and then we'll help figure out what devices or products are needed to accomplish that."

– Anne Ferguson, vice president of marketing, Alarm.com

"New technologies are positively impacting value in the security industry, and we're growing globally in all solution areas."

– Scott Schafer, chairman, SIA Board of Directors

"Bring in cyber experts to penetrate your products before they come to market. The implication of a compromised access control or camera system has a staggering business disruption. Continue to partner with cybersecurity in your own environments and continue to innovate."

– Karen Frank, director of global security, Pratt & Whitney

"I don't see automation replacing people, but it drives the industry to understand that they need to up-level. People need to think about their careers and what's coming, and technology is going to move things in a certain direction."

– Jonathan Aguila, global security director, systems and technology, Facebook

"What gives me joy is to transform the customer experience. What keeps me up at night is making sure products work, are secure and aren't causing any problems."

– Christian Nascimento, vice president, product and premise services, Comcast

"In residential security and monitoring, the technology and response landscape has been changing for years and will only accelerate in the future."

– 2018 SIA Security Megatrends survey respondent

"As an integrator, we are faced with companies asking us how we are going to make their systems secure. In house, we have an IT team that puts together cybersecurity programs and certification for penetration testing. We want to make sure data is safe and secure."

– Erica Mandel, account executive, Schneider Electric

"Integrators are more valuable if they develop a cloud solution. It can make a company more efficient and, over the long haul, more profitable."

– James Rothstein, senior vice president, global security solutions, Anixter

"Private equity money is coming into the space. At least two companies a month in PSA Security are acquired. The only thing that will slow that up is a big giant recession."

– Bill Bozeman, CEO, PSA Security Network

"We have a responsibility around diligence and privacy. The key piece is to get to a proper balance between maintaining privacy and security. It's a double-edged sword; we want to protect the privacy of others but need to know where to strike the balance or provide guardrails."

– Kim Loy, chief product officer, ACRE

"When you're talking about access and identity, maybe we need to simplify. We've taken the concept of 'Do you belong here or not?' and made it much more complicated than that. Maybe we'll see the technology simplify itself to the point where it's more practical to use. In terms of ease of use, simpler is better."

– Daniel Krantz, managing partner, Secure Worker Access Consortium (SWAC)

"The lack of cybersecurity protections for physical security systems could be catastrophic if malware goes there next. We attack this stuff all the time, and it's ALWAYS vulnerable."

– 2019 SIA Security Megatrends survey respondent

"It's interesting how the concept of automation has changed over the years. We have a great opportunity to move products and technologies to enabling a customer experience. The customers don't care what the device is—they want a specific experience."

– Anne Ferguson, vice president, Marketing, Alarm.com

"Today, artificial intelligence is providing insights, but tomorrow it offers autonomy.

– Martin Huddart, head, smart residential, ASSA ABLOY

"Technology isn't the problem; the problem is us. The technology doesn't install itself. We need to look at it from an operational standpoint."

– Brad Hegrat, security principal director, Accenture

"This year, more than any other, all of these Security Megatrends are incredibly relevant to investment in capital and merger and acquisition activity.

– John Mack III, executive vice president, co-head of investment banking and head of mergers and acquisitions, Imperial Capital

"We're transforming from what the traditional brick and mortar offices would look like. How do you design an open office so that people can do their work effectively, and how do you make it secure?"

– Brian Tuskan, senior director and chief security officer, Microsoft Global Security

"Because of phones, sensors have gotten incredibly cheap, which allows us to embed them in so many devices, produce artificial intelligence and serve real human needs. The downside of all that connection is cybersecurity but also complexity. It's almost logarithmic how easy it is to mess with a complex system."

– Gary Shapiro, president and CEO, Consumer Technology Association (CTA)

"We're seeing the demand of convenience driving the security factor. If I'm a consumer, I want to know I can use my phone to enter the business."

– Lee Odess, vice president, service provider business, Americas, Allegion

2020 SECURITY MEGATRENDS

1 CYBERSECURITY IMPACT ON PHYSICAL SECURITY
page 6

2 ARTIFICIAL INTELLIGENCE
page 8

3 FACIAL RECOGNITION
page 10

4 EMPHASIS ON DATA PRIVACY
page 12

5 CLOUD COMPUTING
page 14

6 NATIONAL SECURITY CONCERNS
page 16

7 CONNECTIVITY AND IoT OF EVERYTHING
page 18

8 WORKFORCE DEVELOPMENT
page 20

9 MOVE TO SERVICE MODELS
page 22

10 IDENTITY AS THE NEW PERIMETER
page 24

ALSO INSIDE:

26 Disruption Points for 2020

26 Security Microtrends

MEGATREND 1

CYBERSECURITY IMPACT ON PHYSICAL SECURITY

INDUSTRY NEEDS A NEW WORKFORCE OF ATTACK EXPERTS

TOP OF THE TRENDS IN 2020 IS CYBERSECURITY, just like 2019, and survey respondents resoundingly said it must remain the top trend. From cyber breaks-ins that access residential baby monitors and other Internet of Things (IoT) systems to ransomware rages on public safety departments and private industry, no person, entity or organization is safe.

With new threats coming from every angle and a changing, open connectivity risk landscape teetering on billions of IoT devices, addressing cyberattacks proactively is a major industry undertaking, and it's the number-one concern within the industry, particularly as devices become more powerful and more vital to business processes.

PERSPECTIVES

"Air-gapped systems have been hacked; it's really about having plans for response, and these plans should be practiced. Everyone knows 'Stop, Drop and Roll' and 'Stranger Danger,' but nobody has that type of cybersecurity preparedness."

– Tiffany Pressler, senior manager, HID Global

"As networks and network devices become more sophisticated, large-scale and highly integrated, they present more entry points for potentially damaging access by hackers. As we all know too well, cybersecurity has become an increasingly high-stakes effort."

– Jasvir Gill, CEO, AlertEnterprise

"Cybersecurity requirements are more challenging for mid-size integrators; some may not have resources."

– Bill Bozeman, CEO, PSA Security Network, and Barbara Reeder, CEO/President/FSO, DEFTEC

CHALLENGES

- Finding cyber-ready workers, also closely tied to Security Megatrend 7, workforce development, will be increasingly critical as security executives always ask first: "What are you doing to protect my network?"
- The physical security industry is wrestling with concerns about technology refresh cycles. While new technologies have increased the speed of system refresh cycles, networked physical security systems are still replaced on a slower cycle compared to traditional IT assets, which means aging platforms and unpatched vulnerabilities can exist longer on the network than some chief information security officers (CISOs) are comfortable with.
- Intertwined in this trend are national security concerns (Megatrend 6) being levied by government buyers leery of the lack of cyber protocols for networked cameras and artificial intelligence and facial recognition that gather more data on people than ever before, growing privacy challenges.

STATS

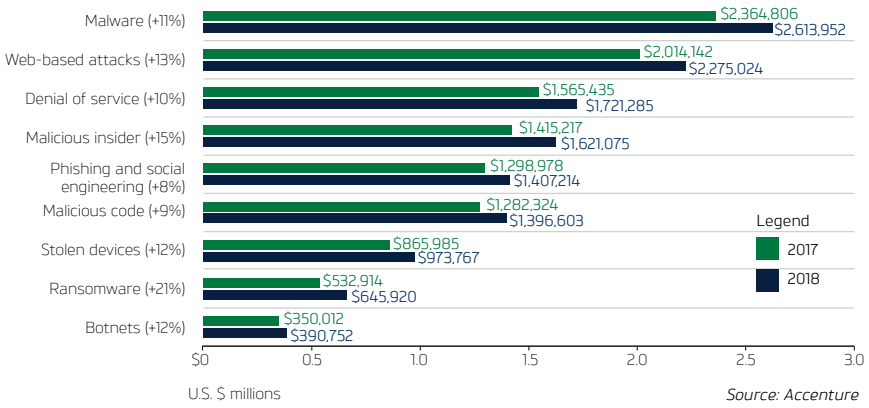
Some 69 percent of enterprise executives believe artificial intelligence (AI) will be necessary to respond to cyberattacks, with the majority of telecom companies (80%) saying they are counting on AI to help identify threats and thwart attacks, according to Capgemini.

DISRUPTION

The primary disruption in the cybersecurity space, as related to physical security, is intertwined with national security concerns (Megatrend 6), as government buyers, corporate customers and integrators are questioning the providence of technology and wondering whether they can trust the firmware and source code supplied.

AVERAGE ANNUAL COST OF CYBERCRIME BY TYPE OF ATTACK

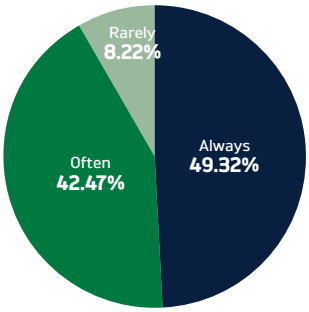
(2018 total = U.S. $13 million)



Source: Accenture

SNG POLL

HOW OFTEN IS CYBERSECURITY OF PHYSICAL SECURITY PRODUCTS A DISCUSSION WITH POTENTIAL CUSTOMERS AND END USERS?



MEGATREND MOVEMENT

Cybersecurity stayed in the number-one position for two consecutive years—2019 and 2020. Encryption is becoming a default, rather than an option, while more and more advanced tools for hacking are commonly available for sale.

TAKEAWAYS

Cybersecurity has become part of the physical security product purchasing decision, where formerly that decision was instead driven by overall product capabilities, specifications, compatibility and pricing.

Chief information officers and CISOs are proactively evaluating the cybersecurity of the devices going on their networks. Encryption is becoming more of a default and less of an option.

Cybersecurity insurance is becoming an important business decision for manufacturers, resellers and practitioners.

More and more advanced tools for hacking are commonly available for sale.

New threats keep surfacing—formjacking on retailers' websites and cryptojacking are go-to moneymakers for cybercriminals.

MEGATREND 2

ARTIFICIAL INTELLIGENCE

AI AND ALL ITS FLAVORS—NEURAL NETWORKS, DEEP LEARNING AND MACHINE LEARNING—ARE A SWEET SPOT FOR SECURITY

AI WILL BE THE MOST TRANSFORMATIVE EVOLUTION IN THE WORLD, let alone the security industry. The always-connected nature of sensors and systems has generated more inputs and data in real time than ever before, and AI promises to make sense of these inputs, whether that's matching faces or correlating security events to trigger response in a global security operations center environment. And while AI offers tremendous potential to improve lives, solve problems and create a better world, the stakes are high and the results can be disastrous if the technology is misused.

In security, it's affecting every part of the market—and over 79 percent of security technology developers and manufacturers at SNG 2019 said that some to all of their product development road maps are tied to AI. On the immediate timeline, AI is working on problems of facial recognition and biometrics and promises to allow video surveillance systems to rely less on human monitoring.

PERSPECTIVES

"It's important to understand the difference between machine learning and artificial intelligence. Machine learning is machines doing different tasks with computer; AI is software that can act without human intervention. That type of automation requires regulation, even to contain it before it can get out of hand. We're still a way off with AI—it's in its early infancy, which gives us a good opportunity to put guardrails in place before it really takes off."

— Tim Palmquist, vice president, Americas, Milestone Systems

"AI is the most disruptive technology until we learn how to leverage it properly. AI has the potential to influence and capture all the different technologies."

— Jasvir Gill, CEO, AlertEnterprise

INFLUENCERS

Artificial intelligence can provide many benefits, including tireless work performance and task efficiency. On the flip side, it can replace human jobs, and it presents the potential for technology to "go rogue." Elon Musk recently called AI "the biggest risk we face as a civilization" and suggested that "we need to be proactive in regulation instead of reactive because by the time we are reactive, it's too late."

STAT

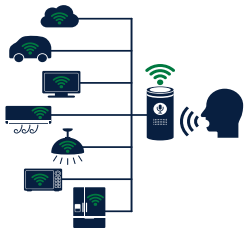
According to a recent report from PricewaterhouseCoopers, AI is set to add $15 trillion to the global economy by 2030 and "has the potential to promote social equity and change society for the better in terms of accessibility."

DISRUPTION

With the transformative power of this technology, AI brings ethical, legal and data privacy issues to the forefront of the discussion.

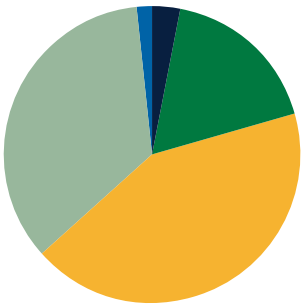
AI IN AUDIO

AI audio and voice recognition is another sector poised to influence the security industry, adding another form of identification. It's also powering advances in language processing, allow humans to communicate with digital systems through voice interfaces, rather than relying on graphical user interfaces or direct programming.



SNG POLL

FOR MANUFACTURERS AND SOFTWARE/SOLUTION PROVIDERS, HOW WOULD YOU CHARACTERIZE YOUR FIRM'S RESEARCH AND DEVELOPMENT INVESTMENTS RELATED TO APPLYING AI TO YOUR PRODUCTS AND SOLUTIONS?



MEGATREND MOVEMENT

It's not surprising that AI has risen to number 2 as a top Megatrend for 2020 over its number-5 spot in 2019. AI is directly driving advancements in the facial recognition and video surveillance markets and provides a needed helping hand in addressing mounting cybersecurity concerns. Part of the digital transformation, AI is advancing identity and credentialing and transcending people and automation processes across the enterprise.

TAKEAWAYS

AI is the underlying advancement behind nearly all technology promises, from automated video monitoring to security data fusion to drones to improved cybersecurity.

AI is directly driving advancements in the facial recognition and video surveillance markets and will also impact robots and drones with self-navigation capabilities and lingual response (chat bots for security applications).

AI will increase applications for situational awareness and make intelligence out of mountains of security data.

The promise of quantum computing's massive processing power would quickly bring AI to the point where it could begin to replicate the power of the human brain (and could crack common encryption standards in a short time).

As the diversity of AI applications grows and as computing power continues to grow and become more commoditized, an increasing amount of AI processing will be handled within edge devices rather than in a centralized, cloud-based environment, according to research firm Tractica.

MEGATREND 3

FACIAL RECOGNITION

FROM BLURRED LINES TO SHARP VISION

RANKED AT NUMBER 3 ENTERS FACIAL RECOGNITION—a resounding response from SIA's Megatrends survey participants—from not being ranked in 2019 to achieving this top tier.

Clear technology advancements are widespread, from identification in security applications to deep consumer adoption though the smartphone. At a technology level, facial recognition has moved from being limited to narrow applications door access and is now becoming a common offering on more general-purpose security cameras at a variety of price points. Growth is being tempered by a strong outcry in the media and moratoriums, bans and other political and public backlashes, which are being countered by the industry.

PERSPECTIVES

"As we work to bring airports into the future, facial recognition and biometrics will be very big things. Once the U.S. starts to move toward a central DMV type of database, you'll see that becoming very big in the U.S., too."

– Erica Mandel, account executive, Schneider Electric

"Facial recognition is really top of mind for me and my company. We want to help as thought leaders and also partners, and there's conversation around how to do that. it's important to understand how the technology works and have a rational discussion, which we haven't seen a lot of in the news."

– Zara Gerald, senior vice president and general counsel, IDEMIA

"What we are seeing is a huge turning point in the way technology is headed. It's about who we are and what we do and fundamental human rights. The thing that keeps me up at night is government cutting off innovation."

– Gary Shapiro, president and CEO, CTA

CHALLENGES

The American Civil Liberties Union wrote in a late-2019 lawsuit that facial recognition software technologies "have the potential to enable undetectable, persistent and suspicion-less surveillance on an unprecedented scale. Such surveillance would permit the government to pervasively track people's movements and associations in ways that threaten core constitutional values." Cities like San Francisco and Oakland, California, banned the technology early on, and recently, Sweden and France prohibited its use in school access control applications.

A graduate student at the University of Toronto and a Massachusetts Institute of Technology researcher revealed problems in facial recognition systems used by various companies. The study found a larger percentage of error in detecting female faces, especially in women with darker skin tones. Taking the bias out of the processing will be critical to mainstream acceptance and deployment.

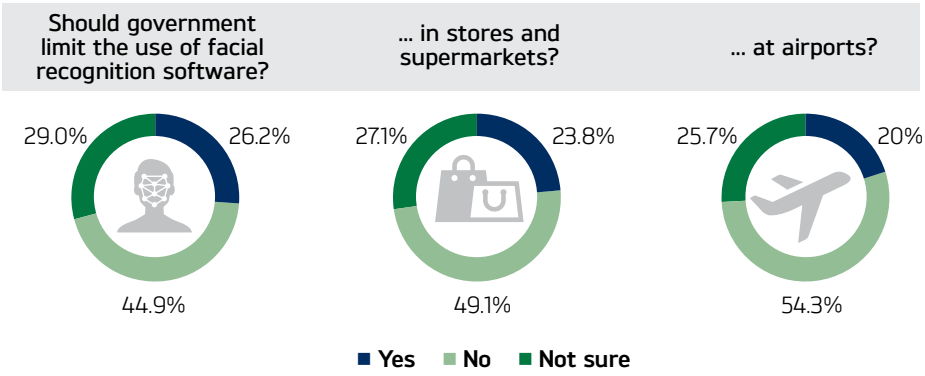
OPPORTUNITY

SIA believes the industry has the opportunity to work together with privacy advocates, legislators and other stakeholders to create best practices, guidelines and effective policy on the reasonable use of facial recognition.

STAT

According to a facial recognition study by Allied Market Research, the market is expected to surpass $9.5 billion by 2022, growing by a compound annual growth rate (CAGR) of 21 percent.

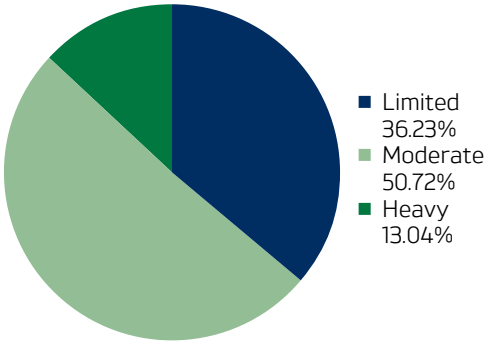
ATTITUDES TOWARDS THE USE OF FACIAL RECOGNITION SOFTWARE (2018)



Source: Center for Data Innovation

SNG POLL

HOW MUCH IMPACT ON THE COMMERCIALIZATION OF FACIAL RECOGNITION DO YOU EXPECT FROM CITY FACIAL RECOGNITION BANS (E.G., OAKLAND, SAN FRANCISCO) AND ANTI-FACIAL RECOGNITION MESSAGING CAMPAIGNS?



MEGATREND MOVEMENT

After not being ranked in 2019, facial recognition catapulted to the number-3 spot in the 2020 Security Megatrends thanks in part to two factors—major advances in technology combined with a wave of anti-facial recognition. With mobile access gaining more momentum and eyes on a friction-free user experience, facial recognition is easing its way into more access control and entry applications. Facial recognition embedded in video surveillance analytics may not be far behind, but privacy and human rights issues are top of mind.

TAKEAWAYS

Massive outcry in the media and moratoriums, bans and other political and public backlashes are being countered by grassroots efforts by security industry organizations and stakeholders.

Watchdog groups have tested facial recognition technologies, and their results have further exposed deficiencies, especially when it comes to misidentifying minority groups—which has obvious negative implications.

With facial recognition deployments, the market is rapidly moving beyond one-to-one access control and entry applications.

MEGATREND 4

EMPHASIS ON DATA PRIVACY

OPEN SYSTEMS, SERVICES AND THE LOT PIQUE PRIVACY INITIATIVES

IT STARTED WITH A SIMPLE WARNING SIGN: You are under surveillance. Now everything you do that creates any data record—whether directly related to your security system or not—is a possible privacy discussion topic. How organizations manage company data, customer data and information from suppliers has created a genuine circle of concern. Data privacy mandates and compliance challenges will introduce new levels of complexity—particularly related to building privacy controls into technology (similar to what social media and big tech had to do), but also relevant to how integrators manage customers' data privacy, especially as solutions become cloud- and software as a service (SaaS)-based.

NEW TECH CREDO

With all the capabilities of open systems, it's important for companies to practice ethical use of technology. Originating in Copenhagen, Denmark, at Techfestival, the Copenhagen Letter is a manifesto calling for the ethical and responsible use of technology. The goal of the letter, which has been signed by more than 5,000 individuals, is to hold tech companies accountable and ensure that humans come before business.

PERSPECTIVE

"Data privacy is an issue everyone needs to be concerned with; it impacts your own data and your products. GDPR is a good guideline and practice moving forward."

– Kim Loy, chief product officer, ACRE

POLICY IMPACTS

It started with the General Data Protection Regulation (GDPR) in the European Union (EU), but that sea change has already come to the United States, with California implementing the California Consumer Privacy Act. The movement of data privacy is affecting security practices related to information and intelligence sharing, too.

DISRUPTION

Smart speakers are now a common ground of breaches—and further heightening consumer awareness of the lack of privacy built into DIY and mass-marketed devices.

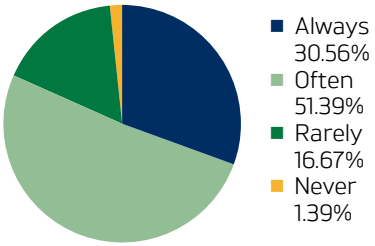
STATS

Gartner predicts $175 billion will be spent on information security and risk management in in 2023, up from an estimated $137 billion in 2019, creating a CAGR of 9.1 percent. Data security, cloud security and infrastructure protection are pegged as the fastest-growing areas of security spending through 2023.

According to the 2019 Definitive Corporate Compliance Benchmark Report, only two thirds of organizations are managing policies and conducting training in cybersecurity, data privacy and confidential information, likely due to flat budgets. Less than half of respondents (46%) have implemented third-party due diligence programs.

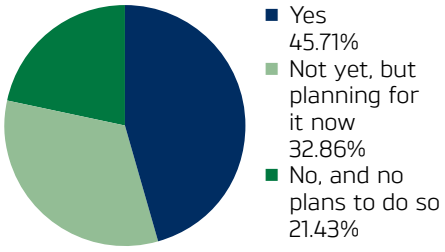
PORTION OF DATA SECURITY BREACHES CAUSED BY INTERNAL EMPLOYEE ACTIONS ...

... AND 83% OF THOSE DATA BREACHES WERE UNINTENTIONAL.



SNG POLL

HOW OFTEN IS DATA PRIVACY A DISCUSSION WITH POTENTIAL CUSTOMERS AND END-USERS?



SNG POLL

HAVE YOU ADDED DATA PRIVACY SPECIALISTS TO YOUR ORGANIZATION'S RANKS?

MEGATREND MOVEMENT

Moving up from its ranking to the fourth spot in 2020 from tallying at number 6 in 2019 is the emphasis on data privacy. With GDPR and numerous other privacy laws that include IoT devices, the open computing environment is causing serious contemplation by consumers and public and private entities.

TAKEAWAYS

General concern across the globe about "big tech" and the implications on privacy will continue to rise. There is a continued emphasis on GDPR beyond the EU with movements underway in the U.S. placing more stringent requirements on data privacy.

We are shifting to an overall emphasis on privacy, not just data privacy.

MEGATREND 5

CLOUD COMPUTING

IT'S A GRAND ENABLER OF INTEGRATED TECHNOLOGIES

"EVERYTHING AS A SERVICE" is what the security industry now is, with software platforms proliferating. The cloud and software-based solutions continue to bring a host of new managed services to systems integrators and new opportunities in access control, video surveillance and integrated system solutions. Security concerns have somewhat tempered, but users remain wary of the overall integrity of their data at on-premises and offsite servers.

PERSPECTIVES

"In the federal government, there are barriers such as mandated bandwidth restrictions. Someone needs to figure out how to package video for the cloud off the shelf for the federal world."

– Wayne Esser, director, National Capital Region Security Forum

"Creating a compliance-ready, hosted IT environment and shifting to the future of security are dependent on having the right people, processes and partnerships."

– Brian Tuskan, senior director and chief security officer, Microsoft Global Security

"There is an awareness issue, misunderstanding about privacy, which limits adoption of the solution in transitioning to cloud from on premises."

– Stuart Rawling, vice president, marketing strategy, Pelco

"At this point, cloud adoption is mainstream. The expectations of the outcomes associated with cloud investments therefore are also higher. Adoption of next-generation solutions are almost always 'cloud-enhanced' solutions, meaning they build on the strengths of a cloud platform to deliver digital business capabilities."

–Sid Nag, research vice president, Gartner

PREDICTION

A mixed approach using cloud, edge computing and on-premises models may continue to dominate over the next several years to address the large base of legacy equipment, especially in access control.

THE PITCH

Compelling reasons to move to the cloud: superior network and system management, better service/support, updating automatically to new versions, more professional physical space and ability to grow the system as needed without forklift replacement.

MEGATREND MOVEMENT

Cloud computing moved down in the latest Megatrends report from number 3 in 2019, overshadowed by new cybersecurity, AI and privacy issues. While lowered just a couple of notches, cloud computing continues to proliferate the industry with new SaaS and managed services models emerging.

$116 billion

Global market size in 2020 for software as a service (SaaS)

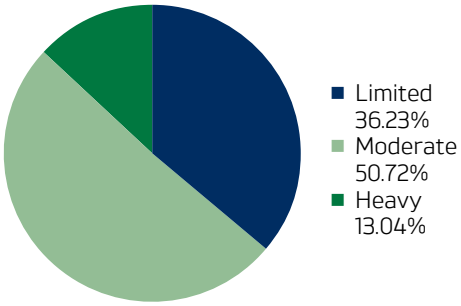
$50 billion

Global market size in 2020 for cloud system infrastructure services, or infrastructure as a service (IaaS)

Source: Gartner

SNG POLL

FOR PRODUCT/SOLUTION DEVELOPERS, HOW MUCH OF AN INVESTMENT ARE YOU MAKING IN THE NEXT 12-18 MONTHS TO MOVE YOUR SOLUTION TO THE CLOUD?



TAKEAWAYS

Even video, long a holdout for smaller systems or with specific recording parameters, now shows more openness to being powered by the cloud.

Hybrid options offering mixed computing, storage and software services environment in on-premises, private or public cloud help migrate security solutions to the cloud.

IT security fears have eased, with traditional longtime on-premises data solutions like Oracle and SAP now embracing the cloud.

Businesses are rallying to develop new offerings or convert existing offerings to cloud services, partly due to improvements in infrastructure and partly due to the positive impact on their business valuations.

MEGATREND 6

NATIONAL SECURITY CONCERNS

TRADE WARS, TARIFFS, PRIVACY AND POLITICAL BACKDROP PROPEL APPREHENSION

THE CHALLENGES ARE VARIED AND DIVERSE. There are state-sponsored hacking and new U.S. government policies about the procurement of security products directly impacting the physical security industry. The connection to AI and facial recognition has reared its head in the form of concerns related to minority bias. Even supply chain security is under the microscope—adding to the complications of distribution and sourcing of products.

PERSPECTIVES

"There are a lot of issues right now that are more complex and increasingly dangerous to the industry, with trade wars and tariffs having a big effect, as well as the issue of modernizing legacy address control in the federal space."

– Craig Sharman, director, federal government relations, Johnson Controls

"The impact of the trade blacklist on the industry will be moderate to high and includes AI and voice recognition system makers."

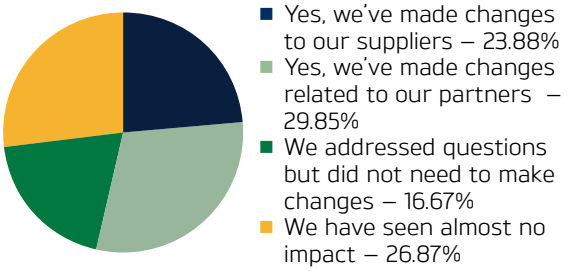
– Steve Surfaro, chair, SIA Public Safety Working Group

STAT

According to The Hill, nearly four in five voters say they will consider presidential candidates' stances on cybersecurity.

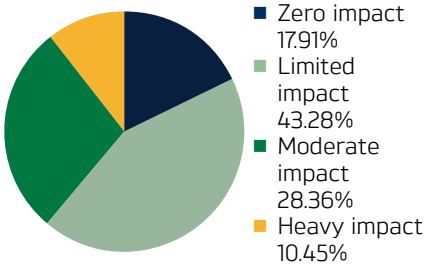
MEGATREND MOVEMENT

On the radar in 2019 as a Microtrend, national security concerns take the number-6 slot on the Security Megatrends 2020 list, stemming from an array or concerns affecting manufacturing, purchasing, procurement and installation. This rise from a Microtrend to a Megatrend follows the impact of the NDAA, which banned specific Chinese companies from being part of federal projects.



SNG POLL

HAVE NATIONAL SECURITY CONCERNS AND/OR GOVERNMENT CONCERNS RELATED TO SOURCING/ SUPPLY CHAIN AFFECTED YOUR ORGANIZATION?



SNG POLL

HOW MUCH IMPACT ARE TARIFFS AND THE TRADE WAR HAVING ON YOUR ORGANIZATION?

TAKEAWAYS

With banned and blacklisted products resulting from the National Defense Authorization Act (NDAA) and Federal Acquisition Regulation rules, will we be seeing the upending of OEM, OBM, ODM and other white-labeling and manufacturing-for-hire types of arrangements for security system components and devices?

Industry organizations and stakeholders need to take quick-step action in stemming the wave of knee-jerk legislation and assert their position on new deployment of technology.

Security integrators need to carefully assess their product channels and how they are addressing concerns and working as a holistic entity within security.

There are concerns that smaller and mid-sized integrators will be squeezed out of projects when the government and security consultants regulate cybersecurity.

MEGATREND 7

CONNECTIVITY & IOT OF EVERYTHING

MORE SYSTEMS, SENSORS AND DATA COMMUNICATE COHESIVELY

THE MEGATREND OF OMNIPRESENT CONNECTIVITY and nearly every device becoming an IoT device is an underlying tech trend shaping nearly all other Megatrends—and has been so for years.

Today, the connectivity of every component means more nuanced features and controls and more opportunity to generate data that can lead to insights, situational awareness and ultimately autonomous actions through the use of AI (Megatrend 2). The dark side is that every device being connected means every device contributes to cybersecurity risk (Megatrend 1).

PERSPECTIVES

"IoT security is the inclusion of inputs and outputs. Input pulls information from the field, and an output is the control. As we expand, we are not just expanding connectivity, but inputs and outputs and our attack vectors are increasing. We need to evolve our operational technologies to address these inputs. Not all IoT devices are created equal. Once we bring physical into the cyber realm, we create a clear and present threat."

– Brad Hegrat, security principal director, Accenture

"Connectivity has evolved in physical security—we're moving from security by obscurity to security by standards."

– Martin Huddart, head, smart residential, ASSA ABLOY

"The exciting part of mobility is that it offers an opportunity to affect the experience in a way we haven't been able to before. With a device comes all the sensors in it, which gives us a greater awareness and can help security be something that's not in your way but something you work with every day."

– Jonathan Aguila, global security director – systems and technology, Facebook

"The next phase for taking advantage of IoT connectivity and services will be moving beyond basic device monitoring and capturing analytics to sophisticated vertical market use case customization and talent needs."

– Will Wise, group vice president, ISC Security Events

CHALLENGE

How do we secure and manage all this data to keep pace with data privacy, cybersecurity and new rules and regulations?

DISRUPTION

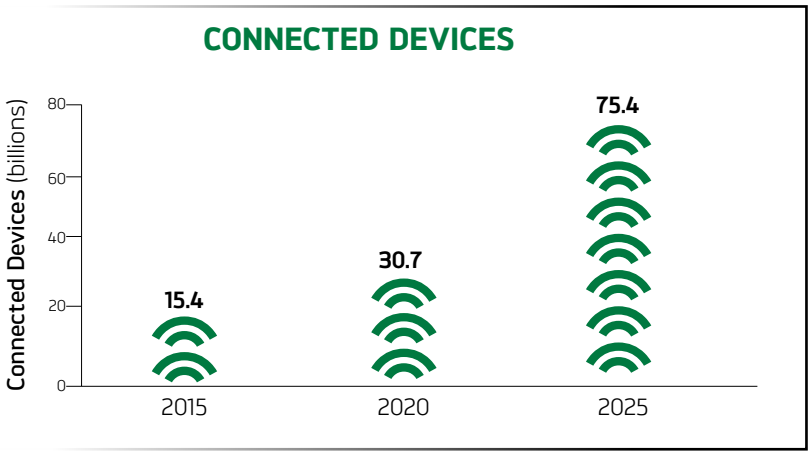
Under the proposed Senate IoT Cybersecurity Improvement Act of 2019 and the National Institute of Standards and Technology guidelines, standards will emerge for federal agencies, contractors and vendors to systematically report and resolve security vulnerabilities for IoT devices.

OPPORTUNITY

The trend of "Connectivity and the IoT of Everything" isn't just about permanently affixed devices; it's also about constant connectivity in the mobile environment.

STAT

According to McKinsey Global Institute, 127 new IoT devices connect to the internet every second. By 2022, 100 percent of the global population is expected to have low-power, wide area network (LPWAN) coverage, driving additional adoption.



Source: IHS Markit

MEGATREND MOVEMENT

Formerly known as "IoT and the Big Data Effect" in 2019, this trend has dropped to number 7 for the 2020 Megatrends. With connectivity a given, new challenges have overshadowed the natural progression of the industry.

TAKEAWAYS

Connected device numbers are booming, but levels of cybersecurity of these devices differ widely.

As IoT expands, we're not just expanding connectivity—we're tripling our attack surface.

It's critical to have integrity inside products themselves—security baked in from the beginning.

Security technology is at the center of all the potential disruption. Sensoring and deployment of security devices create much of the data that can be leveraged to create outcomes for other verticals.

Data recorded from connected devices increasingly analyze processes and identify optimization possibilities.

The proliferation of 5G will further excel and enable connectivity.

Connectivity will intensify the customer experience and find its way to wearable technologies and autonomous vehicles.

MEGATREND 8

WORKFORCE DEVELOPMENT

A TOP BUSINESS GROWTH QUANDARY

UP AND DOWN THE SYSTEMS INTEGRATION CHANNEL, there's a notable need for more skilled workers and an awareness of the new technical side of security coming forth from the merging of physical and cyber disciplines. Systems integrators have new demands for technical skills for their workers, in addition to cyber proficiencies and IT networking.

But the problem isn't limited to systems integrators. Major security technology development firms and security staffing firms are turning to AI-based tools and other innovative hiring practices to identify qualified applicants. Practitioners and supplier partners alike are also finding evolutions in technology and have required them to tap new channels for talent and spin up new outreach programs to attract talent they need.

PERSPECTIVES

"One of the most challenging elements in the security industry today is the ability to attract, onboard and retain talent. Employers of choice are seeking creative ways to create a compelling 'employee experience' which include value-based leadership, cultural diversity, technology solutions to support employees and enhance workflow through automation, whole-health programs, and investing in employee development, to name a few."

– Elaine Palome, director of human resources, Axis Communications

"Labor costs are not going down. We have to embrace technology to provide security."

– Steve Jones, CEO, Allied Universal

"We see and hear it all the time, but the companies that are really winning it are focusing on workforce development."

– Will Schmidt, managing director, Security Lending Group, Pacific Western Bank

STATS

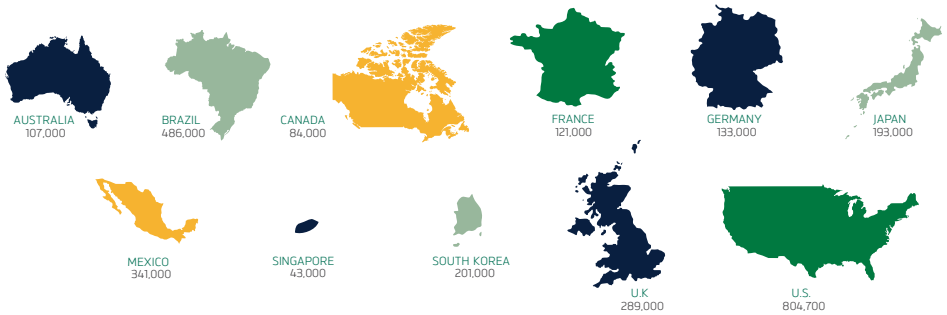
A new study from (ISC)² estimates the current cybersecurity workforce at 2.8 million professionals and estimates that 4.07 million professionals will be needed to close the skills gap.

According to the National Association of Manufacturers' (NAM's) Manufacturers' Outlook Survey, recent research for the second quarter 2019 shows a significant drop in manufacturers' optimism amid uncertainties, softening the global economy and worsening workforce shortage. For the eighth consecutive quarter, the inability to attract and retain a quality workforce remained manufacturers' top business concern. The survey also found that trade uncertainties among manufacturers rose.

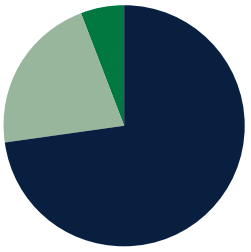
ON THE HORIZON

SIA and the Electronic Security Association are establishing an educational foundation on workforce development to partner in addressing this pressing industry issue.

GLOBAL CYBERSECURITY WORKFORCE ESTIMATES

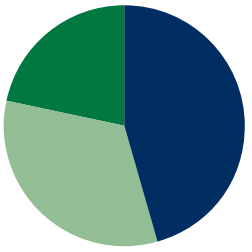


Source (ISC)²



SNG POLL

HAVE YOU ADDED CYBERSECURITY SPECIALISTS TO YOUR ORGANIZATION'S RANKS?



SNG POLL

HAVE YOU ADDED DATA PRIVACY SPECIALISTS TO YOUR ORGANIZATION'S RANKS?

MEGATREND MOVEMENT

Workforce development moved down from the number-4 spot in 2019, landing in the number-8 slot in the 2020 Megatrends forecast. Physical security stakeholders are working on taking control of development of new workers, launching programs in house, recruiting from colleges and universities and partnering with others in the community and organizations to satisfy the need for highly skilled personnel.

TAKEAWAYS

An historically low unemployment rate is magnifying the need for skilled workers.

There's changing demand for skills within corporate security with a stronger IT focus. Guards must also be tech-savvy, as their jobs increasingly piggyback with technology.

The industry is focusing on diversity initiatives—seeking a well-rounded, inclusive workforce to address every part of the channel and highlight the customer experience.

MEGATREND 9

MOVE TO SERVICE MODELS

THE SHIFT ACCELERATES AS USERS EXPECT CONVENIENCE

DIRECTLY CONNECTED TO THE CLOUD TREND, as more security solutions become cloud-based, they move to a service model rather than a product/hardware sales model. For integrators, it's a monumental shift that they are navigating. The evolution started by adding service and maintenance agreements to augment revenues drawn from selling labor and making margins on product, and the next step in the evolution is truly selling security as a service. Such moves change impact on buyers' and practitioners' bottom lines—typically moving such costs from CapEx to OpEx budget lines.

PERSPECTIVE

"We have the opportunity to move beyond just providing products and devices to experiences."

– Anne Ferguson, vice president of marketing, Alarm.com

"Integrators are more valuable if they develop a cloud solution. It can make a company more efficient and, over the long haul, more profitable."

– James Rothstein, senior vice president, global security solutions, Anixter

"It's not the sell, install and run anymore—you're here for the long haul."

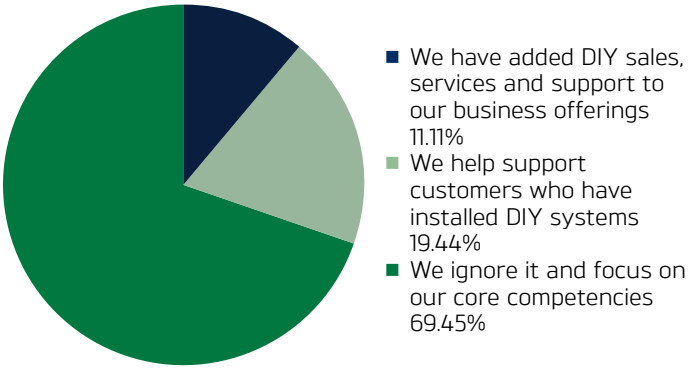
– Scott Schafer, chairman, SIA Board of Directors

"This is such an old story that I didn't realize it was still an issue for you. Amazon is a category killer if you are a retailer. In your category, I don't think Amazon will have the trained installers they need. There is just opportunity for the security industry at this point."

– Gary Shapiro, president and CEO, Consumer Technology Association

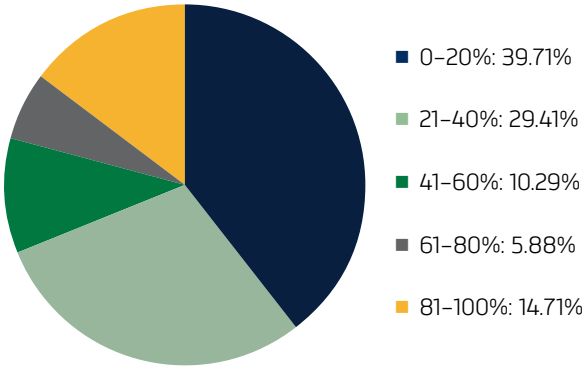
"At the end of the day, it's about consumer choice and giving people what they want. If we make it easy to install, then we have a product that's easy for a professional company to get in and out quickly."

– Mike Harris, president, Ring Solutions



SNG POLL

HOW ARE YOU RESPONDING TO MORE PERVASIVE AND FULLY-FEATURED DIY SECURITY OFFERINGS?



SNG POLL

APPROXIMATELY WHAT PERCENT OF YOUR FIRM'S REVENUES ARE BASED ON RECURRING REVENUE SERVICE MODELS?

MEGATREND MOVEMENT

The move to service models dropped to number 9 in the 2020 Security Megatrends. In 2019 it ranked number 7, shifting only slightly in importance as service providers get a better handle on the future of everything as a service.

STAT

According to Alarm.com, more than 60 percent of consumers who had DIY systems were also getting help from professionals, and more than 80 percent use professional monitoring.

TAKEAWAYS

While the direct-to-consumer/direct-to-business models and DIY product sales models continue to proliferate the industry, security integrators are focusing on professional, exceptional service.

The cloud is a grand enabler, allowing systems integrators to add recurring monthly revenue from new services easily and control and manage all their customers' systems from a single interface.

MEGATREND 10

IDENTITY AS THE NEW PERIMETER

THE CONCEPT OF WHO YOU ARE AND WHAT YOU HAVE GOES MOBILE

WITH MOVEMENT TO THE CLOUD (NUMBER 5 IN THIS YEAR'S REPORT) AND THE TREND TOWARD MOBILITY (a Megatrend in our 2017 and 2018 reports), the perimeter is no longer defined as the corporate campus or the on-premises server room, thus requiring identity to be the new perimeter. Centering on the cloud and SaaS applications, the concept leverages the digital transformation and new identity standards.

According to Forbes, and just like physical security, rapid advances in AI and machine learning are defining cybersecurity's future daily. Identities are the new security perimeter, and zero-trust security frameworks are capitalizing on AI's insights to thwart breaches in milliseconds. Advances in AI and machine learning are also driving the transformation of endpoint security toward greater accuracy and intelligence.

PERSPECTIVES

"It'll get away from managing credentials and toward managing identities—and then you get more awareness."

– Kim Loy, chief product officer, ACRE

"Ultimately, the challenge is who are you, and do you belong here? That's not about a card—it's things about you. And it's dynamic."

– Daniel Krantz, managing partner, SWAC

CHALLENGE

The concept of workforce identity is becoming more complex, with more access rights and roles to manage combined with a more mobile workforce. At the same time, practitioners are still struggling with true integration and automated logic that correlates physical and logical access, all while managing nuanced access to specific resources, environments and data assets.

DISRUPTORS

The large base of legacy access control and the cost to upgrade or migrate to digital technologies is hindering mobile acceptance and stalling identity credentialing development.

Blockchain is starting to look at technology to do employee verification and identification. This will play out largely in the contractor community; linking contractor management technology to security technology will be the next task.

The movement to mobile credentials—with the smartphone as the primary platform—is poised to threaten revenue streams around traditional cards and badges, but that disruption also unlocks opportunity for innovation and new revenue streams.

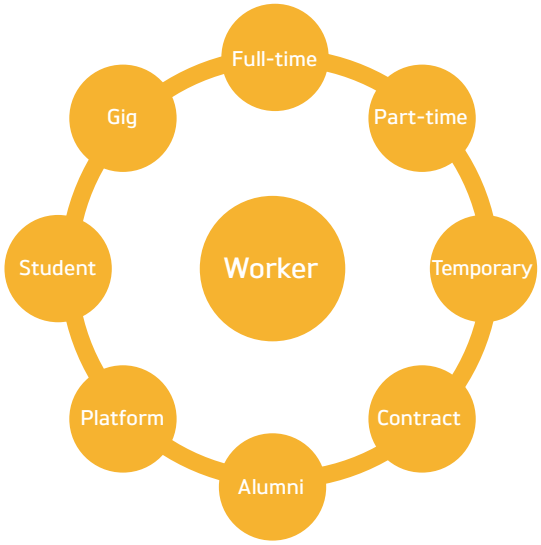
THE CONCEPT OF "EMPLOYEE" IS BECOMING INCREASINGLY COMPLEX

65%

Companies currently rely on external workers for core operations

50%

Amount of work projected to be performed by external works in 2025



Source: External Workforce Insights 2018, SAP Fieldglass & Oxford Economics

MEGATREND MOVEMENT

Identity as the new perimeter is new to our 2020 Security Megatrends, a concept focusing on the individual and the farthest reaches of the protected premises. The concept date back to 2012 and 2013 with IDG and Wired both embracing this concept, but today that forward-thinking idea is really taking effect.

TAKEAWAYS

Trends with identity management moving forward include balancing convenience and friction-free access with appropriate security.

Shifting access control becomes more intelligent and more about situational awareness than just whether someone got in the door or not.

The incorporation of trending human resources functions and software will continue, automating everything from credentialing to off-boarding, on-boarding and even compliance.

Managing identities, not credentials, will be a major shift, with an emphasis on biometrics and multi-factor authentication.

DISRUPTION POINTS FOR 2020

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

1 DISRUPTION POINT: MANNED GUARDING

Just like last year, we predict 2020 will bring additional changes to the manned guarding and contract guard services sector. While guards will have new technologies such as analytics to use to minimize risk and become more efficient, they will require advanced skills, necessitating a more expensive workforce. Robots will play a role eventually, but the technology still needs to be proven.

"There's a lot of opportunity to automate things on premises that people are currently doing manually."

– Christian Nascimento, vice president, product and premise services, Comcast Business

"Whether with drones or robotics, you still go back to the human element. If something's wrong, someone has to respond. The technology will evolve and get better; instead of fighting it, we're embracing it."

– Steve Jones, CEO, Allied Universal

2 DISRUPTION POINT: AGGREGATION OF COMPANIES THAT MANUFACTURE AND RESELL/INTEGRATE

The pie is getting smaller all around. Large and mid-market systems integrators keep buying, and the same is true in both the manufacturing and distribution sides as well as monitoring. This activity is expected to continue into 2020, with private equity funding continuing to stream into the industry.

3 DISRUPTION POINT: DIY AND DIRECT-TO-BUSINESS MODELS

There's more opportunity today to go around a reseller when it comes to product procurement. With DIY models like Ring, SimpliSafe and Arlo readily available, consumers command their own purchasing decisions. In addition, there's growing sentiment in the industry that this type of open-market scenario also causes resellers to lose ground with the end user—who might also go direct to get the products they install.

2020 SECURITY MICROTRENDS

SMALLER BUT INFLUENTIAL FORCES AT PLAY

When we peg our Megatrends, often other influencing factors arise, and this year with the move to integrated, digital networked technologies, there are many confluent forces at work that are tied to our top 10.

- **5G Roll-Out and Increased Broadband Speeds** are closely tied to the cloud and enabling video surveillance and a host of new applications.
- **PSAP Ecosystem Changes** are underway and impacting delivering of alarm/security content to PSAPs/first responders.
- **Mobile Credentials for Access/Identity**—The smartphone will continue to make inroads as the single, friction-free access control and identity device, with advancements coming from wearables. Adoption has been somewhat slow overall, but the promise of 5G connectivity and faster speeds will promote additional applications.

This disruption point is coupled with the market entry of low-cost but well-featured security cameras. These cameras with smart features at low prices are starting to enter the industry; Blink by Amazon, WYZE and others are betting on the consumer's infatuation with video and an "I'll do it myself" attitude.

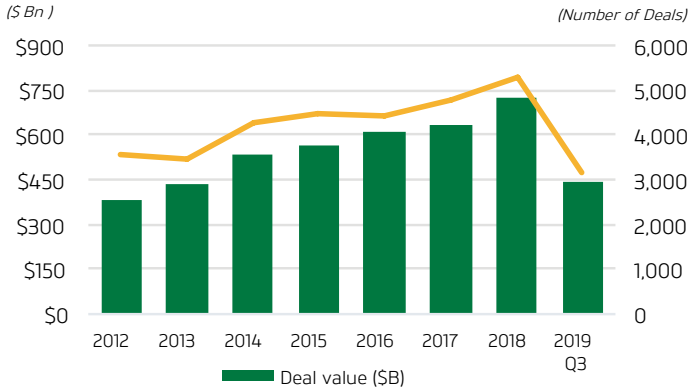
"The direct to business model is cutting the dealer: The aggregation of larger groups that possess both products and services will alter the traditional manufacturer to dealer to end-user model."

– 2019 SIA Security Megatrends survey respondent

4 DISRUPTION POINT: MAJOR VENTURE CAPITAL INVESTMENTS INTO NEW COMPANIES

New equity dollars and investors and new companies: that's the current landscape that could disrupt those unprepared.

U.S. PRIVATE EQUITY DEAL ACTIVITY



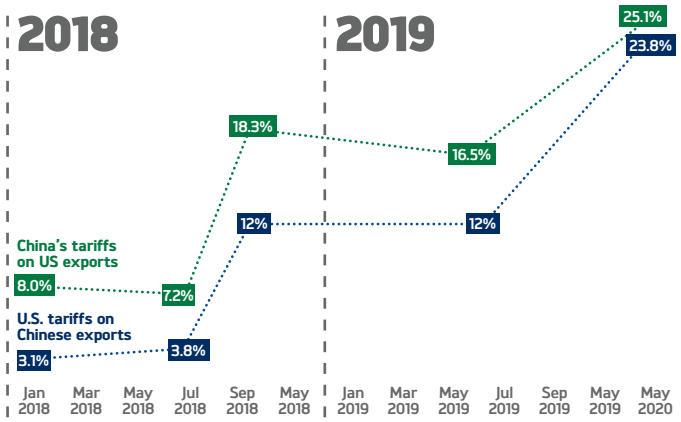
At Securing New Ground 2019, Raymond James' Alper Cetingok forecasted that while 2019 private equity deals were down year over year, 2020 is likely to be a very strong year for private equity investment in the industry due to increasing expectations for an economic downturn.

5 DISRUPTION POINT: GLOBAL ECONOMIC POLITICS, TRADE WARS AND TARIFFS

The political environment is impacting the potential profitability of firms, sending some firms outlooks rising, while causing friction and rising costs in other firms' businesses. With the election year, an impeachment, trade wars and tariffs, anything can happen in 2020, and there is likely to be some volatility in the market.

U.S.-CHINA TRADE WAR TARIFFS

Average tariff rate, percent



Competing tariffs from the U.S. and China have raised concerns of volatility among manufacturers and importers surveyed as part of the 2020 Security Megatrends report.

Source: Peterson Institute for International Economics

- **PropTech**, another digital innovation, is changing the game in real estate. Workspaces are becoming intelligent, adding automation factors to smart buildings. Users can gain more information and data to enhance business processes while increasing safety and adding additional value to integrated platforms.

- **Smart, Automated and Connected Homes**—Consumers expect convenience and a smooth user experience at home, and increasingly, new devices like smart cooking appliances will add to the mix.

- **Increased Demand for Situational Intelligence**—Situational intelligence is the tie that binds: it comes from deeply integrated digital technologies that talk to each other—providing information that proactively reduces risk. Situational intelligence is permeating society—from grassroots such as social media to high-tech surveillance security.

"This is an essential requirement for us in accurately dispatching emergency services, and I think we're seeing the momentum beginning and the AHJs behind us on this."

– Daniel Oppenheim, CEO, Affiliated Monitoring

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