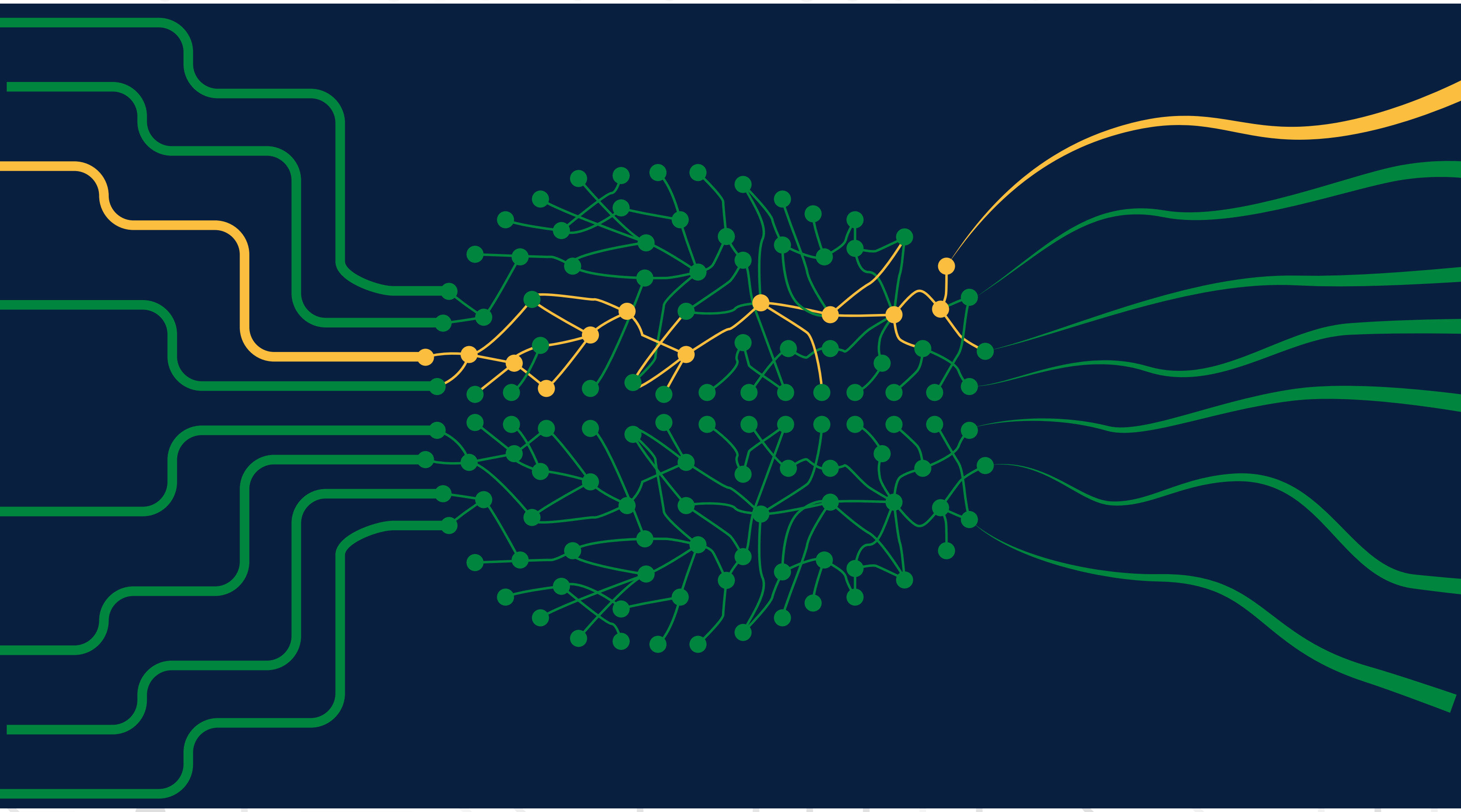
2021 SECURITY MEGATRENDS™

THE ANNUAL VISION FOR THE SECURITY INDUSTRY



STAFF

PIERRE TRAPANESE
SIA Chair of the Board

STEVE VAN TILL
Megatrends Advisor

DON ERICKSON
SIA CEO
derickson@securityindustry.org

GEOFF KOHL
SIA Senior Director of Marketing
gkohl@securityindustry.org

KEVIN MURPHY
SIA Director of Member Services
kmurphy@securityindustry.org

JOHN COLEMAN
Manager, Member Services
jcoleman@securityindustry.org

MARC BENSON
Associate Director of Membership
mbenson@securityindustry.org

KIM LANDGRAF
SIA Manager of Design and Production
klandgraf@securityindustry.org

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

2021 SECURITY
MEGATRENDS™

AN INTELLIGENT FUTURE

The industry's long-term outlook pins hope and progress on the promise of artificial intelligence.

As we present these 2021 SIA Security Megatrends, our goal is to help you align your business with fundamental changes in our industry and thus to remain competitive, prosperous, and profitable, while keeping our world safe and secure.

Now in its fifth year as the industry's defining list of trends, the Security Megatrends report is never a complete erasure of prior trends and subsequent introduction of new trends. We are not chasing the shiny new object. Case in point: You will not see thermal temperature screening identified as a Megatrend.

Instead, we look for longer-term trends and try to measure their importance to our industry and SIA members. Businesses steadily adjust their solutions, services and business models to incorporate these trends and preferences. Over time, these trends' rankings will decrease, eventually falling out of this top 10 report not because their importance to our industry is diminished, but because they naturally become part of how the business of security gets done.

Some trends, however, have more staying power than others. As we noted when we first announced the Security Megatrends 2021 days before our 2020 Securing New Ground executive conference, artificial intelligence (AI) is seen as the resoundingly dominant Megatrend of 2021 and beyond.

AI is the underlying force driving technological advancements in the industry, and will ultimately offer the promise of making security and safety solutions more effective, efficient, responsive and universally available to more users and customers.

The promise to make meaning from the incredible amounts of data generated by our industry's solutions? It comes from AI. The promise to make homes, buildings and cities smarter? Again, AI is the underlying trend that will allow more meaningful advances. The power to incorporate IoT devices such that these products can help us generate action and not drown us in the noise of too many inputs? That's AI, and it's simultaneously influencing cloud computing, data analytics, responsive environments, cybersecurity, facial recognition and many other trends that we recorded in this year's Security Megatrends report.

The report and our outlook is measured and careful. The adoption of AI by the security industry will not happen overnight; instead, it will shape the long-term evolution of security solutions and will be an avenue for growth, competition and creativity for many years to come.

Sincerely,
Pierre Trapanese
Chair, SIA Board of Directors

THANK YOU

SIA THANKS ITS 2020 SNG SPONSORS

ALLEGION

AMAG TECHNOLOGY

ASSA ABLOY
The global leader in
door opening solutions

AXIS COMMUNICATIONS

BOON EDAM

BOSCH

Convergint TECHNOLOGIES
Making a Daily Difference

brivo
simply better security

CyberLink

dormakaba

Genetec

Imperial Capital

PROTOGETIC
The Protective Design Marketplace

Johnson Controls

LENEL:S2

milestone

RAYMOND JAMES

INDUSTRY PARTNER

iSC

MEDIA PARTNERS

SDM

SECURITY
SOLUTIONS FOR ENABLING AND ASSURING BUSINESS

SECURITY BUYER
FOR TODAY'S SECURITY PROFESSIONAL

SIW SECURITY INFOWATCH.COM

SECURITY
News Desk

SECURITY SYSTEMS NEWS
THE SECURITY INDUSTRY'S MOST TRUSTED NEWS SOURCE

SOCIAL MEDIA PARTNER

inside

EXECUTIVE TAKEAWAYS

“At Bosch, we believe in an ‘AIoT’ strategy; that is a combination of artificial intelligence and the internet of things.”

– Tanja Rueckert, CEO, Bosch Building Technologies

“We've seen people that are more and more interested in moving to cloud services. Clients have been asking to have reassurance of moving to the cloud; they're asking a lot of smart questions. For example, what we are doing for security and for reliability, how do we protect their data, what are some of the policies there? So we've been giving our clients a lot of these reassurances, showing them our processes, how we protect their data, how we enable access to systems to help them with the transition to the cloud.”

– Hanna Farah, CTO, Feenics

“Priority number one is standards. We need a change or an enhancement for alarm response standard to accommodate a prioritized response. Prioritized alarms are the future; it's undeniable."

– Donald Young, CIO and EVP of Operations, ADT

“As an industry, we always are trying to put definitions and framework inside a box to make it digestible. We probably owe it to our end users to stop thinking parochially. We have to stop thinking about just security. If we perpetuate security as our only bucket, then that's all we'll ever be."

—Nigel Waterton, Chief Revenue Officer, Arcules

“People will build for futureproof; people will design for automation. There will be sensors everywhere and frictionless and touchless solutions.”

—Alex Housten, Chief Operating Officer, Dormakaba

“Activity levels in the [investing] space should be pretty strong and hold up even if we go into it some sort of near- to intermediate-term economic downturn.”

—Alper Cetingok, Managing Director,
Head of Diversified Industrials, Raymond James

“We should be a business enabler first and foremost.”

– Stephanie Mayes, Synectics

“As businesses continue to maintain a mostly remote workforce, the drive towards the adoption of cloud-based and hybrid solutions will also grow. Relying on the security of trusted cloud partnerships will also support the trend towards zero-trust architecture. Identity management, both user and device identity, will be the linchpin to security. Manufacturers whose systems are capable of adopting this architecture will find themselves at an advantage. Endpoint management is going to be key. Tools that can automate policy compliance at the end-point device will be on the rise.”

—Antoinette King, Key Account Manager, Axis Communications

“Access control has always been touchless, and I think everybody knows that. Everybody who has ever used a card or a fob against a reader knows that they didn't have to physically touch that reader with their fingers, so let's be real about that; it's only more touchless.”

—Steve Van Till, President and CEO, Brivo

“The bull market continues, but it’s a little harder to say that it's reasonable to expect that to be sustainable, given the kind of challenges we're going to have in the economy, given the pandemic. Private equity deal flow, which has steadily increased for the last few years, will undoubtedly have a meaningful pullback.”

—John Mack III, Executive Vice President, Imperial Capital

“Change is outpacing the production of competent professionals, which means that AI is more an art form than a science. The lack of a common language among all parties remains as a barrier to scalability, as does how specific and narrow most AI skill sets remain.”

—Gartner, “Top Strategic Predictions for 2019 and Beyond”

HOW WE PRODUCED THE 2021 SIA 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, SIA 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 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. A special poll-driven session on the second day of SNG 2020 provided additional feedback related to the Security Megatrends and helped generate some of the chart data included in this report.

Through SIA's 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 2021 SIA Security Megatrends report, but also provided you insights and action items to facilitate a successful future in the security industry.

2021 SECURITY MEGATRENDS

ALSO INSIDE:

MEGATREND 1

ARTIFICIAL INTELLIGENCE

IN 2020, WE WROTE: "AI WILL BE THE MOST TRANSFORMATIVE EVOLUTION IN THE WORLD, let alone the security industry." In the 2021 report, it's no surprise that AI has become the dominant Security Megatrend. AI is the underly technology change behind so many of the over Megatrends identified in this report. Predictive data analytics (#3 in this year's ranking) is intelligence applied to seeking meaning out of mountains of data. Facial recognition (#7 in the 2021 ranking) is AI applied to matching of faces. Responsive Environments & Intelligent Spaces (#8 in the ranking) may be driven by rules engines, but at its most complex, when dealing with high complexity and many inputs, then these responsive environments must be powered by AI.

However, there's one caveat, and it's that AI is truly an aspirational trend. AI is that application of logic, rules and understanding that is always one step ahead of where we are now. What we may call AI today is likely to be seen as a normal feature in the future. Something considered AI in years past like object tracking in video surveillance, today is just a normal feature of a smart video security system. Each time a feature is achieved, the AI bar is raised, such that "real AI" always lies just beyond our current grasp.

PERSPECTIVES

"If you look around, AI is transforming nearly every industry: PropTech, healthcare, retail, automotive, marketing and FinTech, to name just a few. We don't see that happening yet in security, but I think we're on the cusp, and that the results will be dramatic."

– Steve Van Till, President and CEO, Brivo

"One area of interest that we are seeing at a high level is the kind of modification and repurposing of existing analytics and AI for things like facemask detection, social distancing, heat mapping, people counting and contact tracing. Interest level is very high, but whether this translates into a significant market penetration in the future remains to be seen."

– Jason Oakley, CEO, North American Video

NEAR-TERM APPLICATIONS

In the immediate future, AI within physical security will be in the form of specialized systems that apply AI to one or very few applications, but in the future, systems are likely to incorporate many AI-powered features.

- AI-powered facial recognition
- AI for video surveillance and tracking
- Environment-responsive drones and robotics
- Voice-responsive or voice-assisted security systems
- Synthesizing patterns or trends from large arrays of data

NEXT-LEVEL AI

While near-future AI is about matching, recognizing, tracking, processing and navigating, as AI advances, the movement is clearly toward systems that can do all of the former and then also apply decision-making to support truly autonomous systems. Picture a video surveillance system that detects someone climbing a perimeter fence, pans other cameras to this area, alerts the guard response team, deploys a drone to track the suspected intruder, and changes the access control system to a more restrictive level given the increased risk.

ANOTHER NEXT FOR AI

A particularly savory dream for video surveillance systems is applying near-future AI features like facial recognition and person/object recognition and classification in crowded environments. Want even more of a challenge? Perform all these features in real-time.

STATS

54 PERCENT

Global growth expected in the AI software market in 2020, rising to a global market size of $22.6 billion.

Source: "Artificial Intelligence Software Market Growth Forecast Worldwide 2019-2025," Statisa, August 2020

$267 BILLION

Expected global market size for artificial intelligence in 2027

Source: Fortune Business Insights, 2020

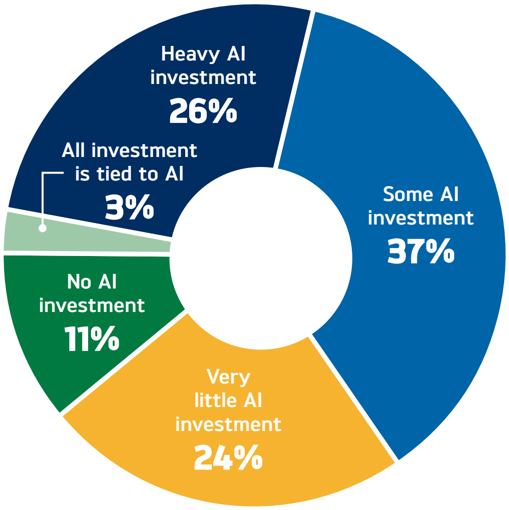
CHALLENGE

The challenge will be trust as AI adoption spreads. An IBM report noted that systems that demonstrate bias can significantly erode trust in AI systems. To build trust, the study noted that information about how these AI technologies work and how they make decisions must be very open to the public.

SNG POLL

HOW WOULD YOU CHARACTERIZE YOUR FIRM'S RESEARCH AND DEVELOPMENT INVESTMENTS RELATED TO APPLYING AI TO YOUR PRODUCTS AND SOLUTIONS?

Compare this to data points from Informa Tech's study of North American companies, which found that 36% were in the developmental stage, while 30% were in an advanced stage with multiple AI applications in production.



MEGATREND MOVEMENT

Ranked second in 2020 and fifth in 2019, artificial intelligence jumped to the number one spot in 2020 as this trend was perceived as the trend that would ultimately drive most technology advances in coming years.

TAKEAWAYS

AI is always the thing around the corner. If your system can do that complicated task today, it's not considered AI (even if that task requires great computing intelligence).

As AI advances, solutions will progress toward autonomous responses that require processing even more complicated situations.

Most technology/software/product developers in security are already applying AI to their solutions, or at least have R&D programs that will put AI into their roadmap.

MEGATREND 2

CYBERSECURITY FOR PHYSICAL SECURITY

THE AI-CYBER CONNECTION

"[C]oncerns have been raised that using AI for offensive purposes may make cyberattacks increasingly difficult to block or defend against by enabling rapid adaptation of malware to adjust to restrictions imposed by countermeasures and security controls."

"Increasing dependence on AI for critical functions and services will not only create greater incentives for attackers to target those algorithms, but also the potential for each successful attack to have more severe consequences."

Source: The Brookings Institute, "AI Governance" report series, author: Josephine Wolff, Assistant Professor of Cybersecurity Policy, The Fletcher School, Tufts University

IF THE TOP TREND FOR 2021 IS AI, then what is biggest concern organizations have about AI acording to Inform Tech's 2020 report on the State of Artificial Intelligence?

You guessed it: Security. And more specifically, how to keep these intelligent systems secure from a cybersecurity standpoint. After all, the more powerful systems become, the more of a prize they become in terms of potential business disruption or being used for criminal or other illegal activity.

PERSPECTIVES

"Our industry is trying to find its way relative to what role we play in in helping our clients with cyber security. I don't think that we ever looked at ourselves or our industry as being cyber security experts, but rather, the question becomes 'How do we a make sure that we're not a vector into our customers site?'"

– Mike Mathes, Executive Vice President, Convergint Technologies

"With the advent of AI, machine learning, 5G and edge computing, you're going to see an increasingly complex technology landscape, not just by virtue of the technology but by the rate of change of technology and the new types of business models that these technologies open up, and I think cybersecurity is going to become very complex."

– Kurt John, Chief Cybersecurity Officer, Siemens

COMMON THREATS & PHYSICAL SECURITY

Ransomware: The application of malicious code to extort a system owner (often for money) by limiting the owner's access to their files/systems.

Example: *In 2017, a ransomware attack affected the Washington, D.C., camera system, just a week before the scheduled presidential inauguration (Good news: The timing was not believed to be intentional, and D.C. recovered control of its system without paying the ransom).*

Malware: Software/code used to gain unauthorized access or cause damage to a computerized system.

Example: *Malware on machines running critical security systems, allowing hacker to attack that system or siphon information through unauthorized backdoors.*

Social Engineering: Using deception or using weakness within common social responses (e.g., courtesy, quid pro quo, etc.) to convince a person to reveal otherwise secured information.

Example: Something as simple as "tailgating" through a door applies social engineering to the physical environment.

Phishing: Phishing is often considered a subset of social engineering and is commonly presented as deceptive emails used to obtain sensitive data. It is usually referred to as spear-phishing when the target or the data desired is very unique, and thus aimed at a single individual or a very limited audience of users.

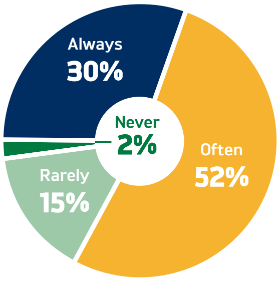
Example: Phishing employees to reveal login credentials to critical physical security technology systems.

43% of cyber attacks target small businesses

Source: Small Business Trends

SNG POLL

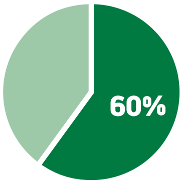
HOW OFTEN IS THE CYBERSECURITY OF PHYSICAL SECURITY SOLUTIONS/ SERVICES A DISCUSSION WITH POTENTIAL CUSTOMERS AND END-USERS?



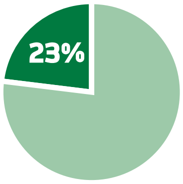
THE RISING COST OF CYBERSECURITY

Cost increases across 17 components of cybersecurity protection over the last two years. (*Source: Accenture, "Third Annual State of Cyber Resilience," 2020*)

Percentage of organizations reporting security component cost increases of up to 25%



Percentage of organizations reporting security component cost increases of more than 25%



Security Components Ranked by Biggest Cost Increases

1. Network security
2. Threat detection
3. Security monitoring
4. Cyber risk management
5. Firewalls
6. Threat intelligence
7. Application security
8. End-point detection and response
9. Incident response
10. Identity and access management
11. Vulnerability management
12. OT-related security
13. Privileged access management
14. Staffing (or People)
15. Remediation
16. Governance, risk and compliance
17. SIEM and event consoles

GOOD NEWS?

The same Accenture report noted a 27% reduction in the average number of security breaches in 2019; organizations studied faced 22 security breaches, a decrease from 30 in the prior year.

MEGATREND MOVEMENT

Cybersecurity for physical security has been a leading Security Megatrend in recent years, and while it may not have retained its crown position in 2021, it is by no means fading. The criticality of security systems keeps it top of mind, as do high-profile incidents like ransomware attacks on government data systems.

TAKEAWAYS

Cybersecurity continues to be a rising cost for businesses.

The concern among business leaders like integrators and manufacturers, whose systems are being added to customers' networks, is that they "do no harm" by creating new cyber risk for their clients.

People are the threat vector. Social engineering and phishing are among the most common methods used to gain access to systems, thus allowing implanting of malware, ransomware or other malicious code.

The importance of cybersecurity has created an entire new class of service and solution providers – companies which provide IoT device security services specifically for physical security devices and systems.

MEGATREND 3

PREDICTIVE DATA ANALYTICS

THE DIGITALIZATION OF EVERYTHING MEANS MORE DATA. According to DOMO's "Data Never Sleeps 5.0" study, 2.5 quintillion bytes of data are generated each day, and 90 percent of the data in the world was generated in the last two years.

Video, of course, is among the largest generators of data. A study by Wikibon reported that video surveillance generated nearly 39 zettabytes of data in 2018, more than any other category of data generating systems, and was growing at a furious pace of 42% compounded annual growth rate. In the world of security, every card read, every motion detection, every audio feed is generating data, but the usefulness of that data comes from the potential to process it.

Enter AI again (the #1 Security Megatrend for 2021). Computer processing power promises to reveal insights from all of this data and then apply those insights to business or security. Can you use video and access systems' data together to determine when your facility is at most risk for tailgating? Can the mountains of data generated by a video surveillance system tell you about your customers habits and typical movements or allow you to design more productive environments for employees? What patterns can be found and what predictions can be made?

PERSPECTIVES

"This is the holy grail: Being able to amass enough data to be able to predict what might happen next."

– Steve Van Till, CEO and President, Brivo

"AI and analytics help us make sense of data, because raw data is not really useful; it's not helpful, so you need analytics to create a dashboard, to create reporting and to create insights. And if you want intelligent insights, you use artificial intelligence and machine learning and algorithms that use deep learning that helps you identify patterns [in the data]."

– Tanja Rueckert, CEO, Bosch Building Technologies

"In effect what Big Data should really stand for is SMART Data and whilst I think the term Big Data will disappear in time, the increasing production and use of SMART Data is definitely here to stay."

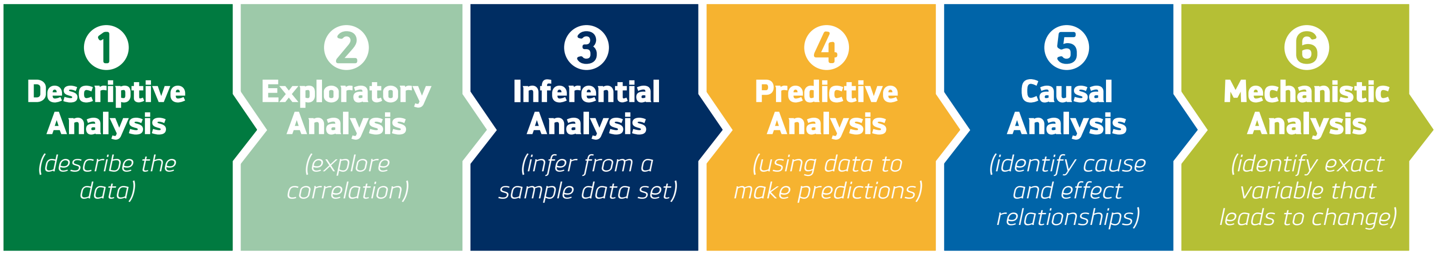
– Author Bernard Marr in his book "Big Data"

"That's always been the challenge: We don't want to be crushed by data."

– Mark Duato, Executive Vice President, Aftermarket, ASSA ABLOY Opening Solutions

THE SIX TYPES OF DATA ANALYSIS

As taught in the Johns Hopkins University course "Data Science Specialization," there are six steps to fully performing data analysis:



1. **Descriptive Analysis** *(describe the data)*
2. **Exploratory Analysis** *(explore correlation)*
3. **Inferential Analysis** *(infer from a sample data set)*
4. **Predictive Analysis** *(using data to make predictions)*
5. **Causal Analysis** *(identify cause and effect relationships)*
6. **Mechanistic Analysis** *(identify exact variable that leads to change)*

CHALLENGES

With the mountains of data generated given the overall proliferation of IoT devices, the challenge the industry now faces is that it is actually easier to create data than to deeply process it to generate meaningful insights.

The lack of consistent meta data being generated by the different video surveillance systems has been a frustration point, according to an engineer working on AI problems for one major chip maker we spoke with.

THE SOLUTION

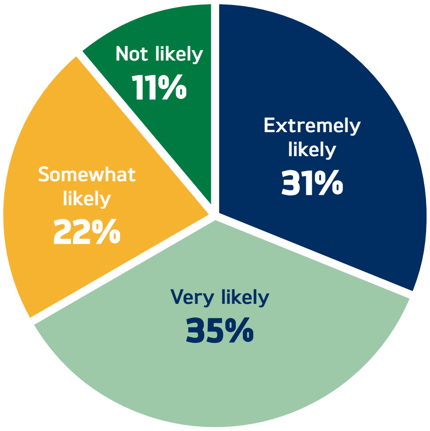
Yet again, advances in artificial intelligence offer promise here. Advanced computing power is required to make sense of those mountains of data, and artificial intelligence has the potential to also process video and autonomously add the requisite meta data such that video from multiple different systems and cameras can be used consistently in data analysis. It's fair to say, this entire Megatrend is built on the potential of AI applied to big data.

APPLY TODAY

Being able to predict incidents may indeed be the holy grail, but many point to practical data insights like when predictive maintenance is required as a much more achievable short-term goal.

SNG POLL

DO YOU THINK PREDICTIVE DATA ANALYTICS WILL BECOME A MEANINGFUL FEATURE WITHIN YOUR PRODUCTS, SOFTWARE OR SOLUTIONS WITHIN THE NEXT 2 YEARS?



MEGATREND MOVEMENT

While not specifically called out in the 2020 report, this Security Megatrend has roots in the #2 2019 Security Megatrend, "IoT and the Big Data Effect." In 2021, those trends have separated, and respondents to the annual Security Megatrends research survey identified predictive data analytics as a separate trend from the Internet of Things.

TAKEAWAYS

AI is necessary for advanced analytics applied to high volumes of complex data.

Predicting the problem before it happens is the ultimate goal of data analysis.

Nearly two-thirds of SNG attendees said that predictive data analytics will be a meaningful feature of their solutions within two years.

MEGATREND 4

CONNECTIVITY AND THE IOT OF EVERYTHING

A long-standing trend that defined the future of today's security technology industry, this could be the last year "connectivity and the IoT of Everything" will be identified as a trend in this report, because the reality of the security industry is that today, nearly every single solution, device or sensor our industry employs is an endpoint IoT device.

So why does it still rank in 2021? We would point to the massive installed base of legacy equipment that will eventually convert into networked, IoT-based solutions. The move from legacy devices to IoT devices will either come during normal product lifecycle replacements, major facility improvements or when the new value from a networked device overcomes the stasis that would keep antiquated but functioning technology in place.

PERSPECTIVES

"We know that there are close to 30 billion IoT devices on the network right now, and the number is going to be growing next year. So that gives you a perspective of the number of endpoints that are threatened by the all the hackers that are out there."
– Min Kyriannis, Managing Director/Founder, JMK Group

"These data collection devices are meant to go ahead and paint pictures of what's going on with my elderly parents, what's going on with my front door and my garage and are they open or closed, what's going on with an endless list of things. Our detection devices are becoming more capable and sophisticated of telling us more specifically and more accurately what's going on."
– Donald Young, CIO and EVP Field Operations, ADT

"Right now, we have roughly 4 billion servers on the Internet, but that's not where we're deploying new stuff. We're deploying new stuff in IoT, and we expect in the next maybe 20 years that there will be 40 billion IoT devices."
– Pierre Racz, President and CEO, Genetec

STATS

41.6 BILLION
Connected IoT devices in 2025

79.4 ZETTABYTES
Amount of data those devices will generate in 2025

Source: International Data Corporation (IDC)

AI IMPACT

Gartner predicts that by 2022, AI will be part of more than 80 percent of enterprise IoT projects. Already there is strong pervasiveness of AI in IoT. As Deloitte noted in a report for Wired Magazine, "Machine learning for predictive capabilities is now integrated with most major general-purpose and industrial IoT platforms, such as Microsoft Azure IoT, IBM Watson IoT, Amazon AWS IoT, GE Predix, and PTC ThingWorx."

THE CYBERSECURITY CHALLENGE OF IOT

More IoT devices equals more potential endpoints to attack, and most buyers of IoT devices in home environments are overestimating the security of these devices according to a study from the National Cyber Security Alliance (NCSA). The problem, says SC Magazine, is that "IoT devices, particularly those that are cheap, outdated and hard to upgrade, are widely considered to be an easy target for hackers."

RELATED TRENDS

1 AI

3 PREDICTIVE DATA ANALYTICS

8 RESPONSIVE ENVIRONMENTS AND INTELLIGENT SPACES

5G, WIRELESS COMMUNICATIONS AND THE IOT

To support the over 41 billion installed IoT devices forecasted by 2025, the method of connecting that many devices will be through multiple wireless technologies, like 5G and ultra-wideband. A 2020 McKinsey & Company report on 5G identified three strong growth areas for 5G IoT use cases:

1 Enhanced mobile broadband (EMBB), particularly with relevance for ultra-HD video streaming

2 Ultra-reliable, low-latency communications (URLLC) for control of critical devices (examples: robots and drones)

3 Massive machine-type communication (MMTC) for the "automatic generation, transmission and processing of data among numerous machines with little to no human intervention."

Source: "The 5G Era: New Horizons for Advanced Electronics and Industrial Companies," McKinsey & Company

MEGATREND MOVEMENT

When SIA's Security Megatrends first edition report was launched in 2017, IoT was the number one trend. Last year it was ranked #7, and we saw it rise to #4 in 2021. The rise in ranking is believed to have been driven by AI advances that promise to make IoT devices for security much more than just "basic sensors." When the data that these sensors and devices generate can be processed using AI (Megatrend #1) to create predictions from the data (Megatrend #3), then there is even more value produced by these connected devices.

TAKEAWAYS

IoT for security will be part of a global technology trend that propagates more and more IoT devices.

These IoT devices are likely to become more powerful overtime, offering the processing power of AI at the edge rather than requiring a central system to perform the processing.

Expansion of IoT devices requires expansion of wireless communications systems.

Continued rapid expansion of IoT devices means more potential cybersecurity risks.

MEGATREND 5

CLOUD COMPUTING

Let's admit it: 2020 was the year of the cloud. Companies that delivered cloud-based solutions for security generally said they experienced a positive year, as the move to mobilize workers during the pandemic had buyers discovering more value from the use of cloud-managed or cloud-powered systems. In the general business world, companies that delivered cloud systems saw their valuations soar (think Zoom), while those which delivered on-premises systems worked rapidly to introduce cloud features and cloud access.

Even dedicated cloud solution providers admit, however, that the security industry lags in adopting cloud solutions, and concerns, whether unfounded or not, center around the cybersecurity and resilience of cloud systems that are used for a business' critical safety and security functions.

PERSPECTIVES

"There's a lot of white space and opportunity to grow organically in this business. The use of new business models – SaaS and cloud computing and analytics – are incredibly applicable and are going to drive a lot of opportunity."

– John Mack III, Executive Vice President, Imperial Capital

"In other industries like banking and healthcare, the [cloud] trends have picked up sooner than the security industry where a lot of the information and a lot of the systems [in those industries] have moved to the cloud. Moving to the cloud means not only having remote access to the system, but really to take the benefits of the cloud, which has the security, the reliability and the redundancy that the cloud offers."

– Hanna Farah, CTO, Feenics

"This industry evolved to in order to secure buildings and secure assets and those systems had to be secure. That was the primary purpose, but as we move forward, these systems don't get swapped out in the way that we throw away our mobile phones and buy the new technology so we can access the cloud services. It doesn't work that way. We're seeing an evolution towards cloud services."

– Pauline Nordstrom, CEO, Anekanta Consulting

"Transition to the cloud isn't the magic pill that solves everything, but it's certainly going to reduce risk overall of these systems."

– John Deskurakis, Chief Product Security Officer, Carrier

STATS

59 PERCENT

Portion of of tech buyer respondents who said they would be mostly or all in on the cloud within the next 18 months

32 PERCENT

Amount of of the survey respondents' organizational budgets that are being spent on cloud computing

Source: IDG 2020 Cloud Computing Survey

CLOUD BENEFITS

- Redundancy, reliability and recovery
- Centralized updates
- Centralized security management
- Scalability and Speed-to-scale
- Enables mobility

LINGERING CONCERNS

- Data privacy
- Cybersecurity
- Data retention
- Partner/vendor trust
- Performance, bandwidth and connectivity

A MINDSET SHIFT

"There still is a major risk in cloud computing. The shift in mindset isn't believing that cloud computing is safer; the shift in mindset is that businesses are willing to take the risk to go into the cloud under the circumstances that we are presented. There is an obscurity in cloud computing that either businesses don't understand or are taking the risk for it. If there is a data leak, the account holder is still liable, unless it is clearly stated in their contracts that any data breach is owned by the company who is running the service." – Min Kyriannis, managing director, EMD JMK; chair, SIA Cybersecurity Advisory Board

WHO'S RESPONSIBLE?

Shared Responsibility Model for Security in the Cloud

On-Premises *(for reference)*	**IaaS** *(infrastructure-as-a-service)*	**PaaS** *(platform-as-a-service)*	**SaaS** *(software-as-a-service)*
🟦 User Access	🟦 User Access	🟦 User Access	🟦 User Access
🟦 Data	🟦 Data	🟦 Data	🟦 Data
🟦 Applications	🟦 Applications	🟦 Applications	🟩 Applications
🟦 Operating System	🟦 Operating System	🟩 Operating System	🟩 Operating System
🟦 Network Traffic	🟦 Network Traffic	🟩 Network Traffic	🟩 Network Traffic
🟦 Hypervisor	🟩 Hypervisor	🟩 Hypervisor	🟩 Hypervisor
🟦 Infrastructure	🟩 Infrastructure	🟩 Infrastructure	🟩 Infrastructure
🟦 Physical	🟩 Physical	🟩 Physical	🟩 Physical

🟦 Customer Responsibility vs. 🟩 Cloud Provider Responsibility

MEGATREND MOVEMENT

Cloud Computing held onto its fifth-position ranking from the 2020 report, and the continued ranking of this Megatrend (which was in our first edition report from 2017 as #7) is no surprise given the steady growth of cloud solutions in the security industry during the 2020 COVID-19 pandemic.

TAKEAWAYS

Cloud market has been positively influenced by the move to work-from-home that was driven by the pandemic.

Adoption of cloud solutions for security has been growing rapidly because buyers are willing to accept the risks in exchange for the benefits of convenience.

Cloud-based solution providers are still having to overcome objections around security and reliability/resilience of cloud systems compared to on-premises solutions.

Industry has seen strong cloud adoption among residential security and smart home automation providers.

Cloud offers new income streams for integrators and is closely related to the "Move to Service Models" (Megatrend #10).

MEGATREND 6

TOUCHLESS & FRICTIONLESS SOLUTIONS

While the security industry has long aspired to frictionless solutions, particularly in the area of facility access control, the touchless element of this 2021 Security Megatrend was what made all the difference – driven obviously by the global health emergency and health officials' recommendations to limit contact with surfaces.

Fortunes of a number of SIA member companies that had touch-free solutions (optical turnstiles, automatic door openers, and other contactless/touchless equipment) were bolstered by the health concerns, and any solution that allowed a distance-based approach saw even more value in 2020. An example was the dramatic rise in thermal temperature scanning systems.

We asked a leading manufacturer of automatic door openers if the pandemic had indeed led to greater sales of those devices, and the CEO said that they were "selling door actuators as fast as we can make them," but he noted the increased sale of the devices was being influenced by high-end clients and specialized customer environments like government facilities which had to keep personnel in the office for security reasons.

PERSPECTIVES

"We've seen a lot of change in perhaps what I would call the lobby experience, the portal: The rush to do temperature testing, the rush to move away from contact technologies, the rush to explore biometric technologies like facial recognition or other types that are that don't require you to touch anything as you progress through into the building."

– Howard Johnson, CEO, AMAG

"When I look at touchless and frictionless access, I don't think that's going to go away [after the pandemic]. It's really been in our market for decades. Through automatic sliding doors, detection/presence sensors, biometrics, that's all been there. It's only going to become more heightened and growing in the post-pandemic world."

– Valerie Currin, President and Managing Director, Boon Edam Inc.

"By far the research is showing they [users] would rather be in an environment where they are coming into little to no contact with any kind of door handles. ... Touchless solutions and frictionless solutions are a tremendous opportunity for us collectively as an industry. The data showed from market research that it's going to grow to 16-18% CAGR through 2025 – that's on a global basis; different regions of the world are ready with their infrastructure to adapt at different levels."

– Joe Hudock, Senior Vice President of Marketing, dormakaba USA

"Frictionless and touchless has been around for years; the tools have just been expensive. Will organizations change their hardware to make it happen? Is it the top 1% or is it the 99% of others?"

– Nigel Waterton, Chief Revenue Officer, Arcules

LOSING TOUCH

Losing touch can be a good thing for once. The move to touchless is being seen in these six technology solution areas, among others.

- Wave-to-open door control switches
- Touchless biometric solutions
- Automatic door operators
- Temperature screening
- Mobile credentials
- Phone-based visitor management

PHONE AT THE CENTER

The mobile phone continues to be the central tool to unlock the "frictionless" side of this trend, but at least as adoption grows, phone-based frictionless access control will likely remain only an option, side by side with card type access, much as the way that keyed access is often still available in facilities with electronic access control.

BENEFITS

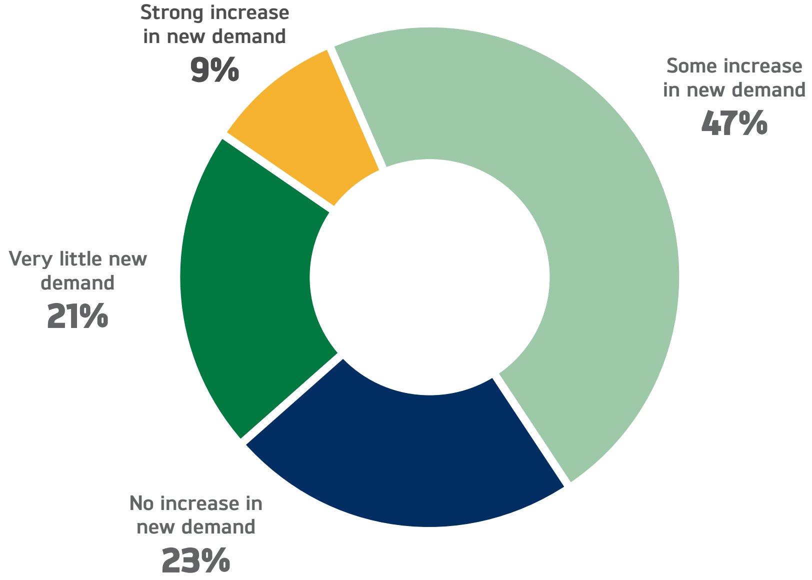
- Phone is almost always with users
- Built-in communications technologies (e.g., Bluetooth, WiFi, NFC)
- Biometric options often built in
- Can support multi-factor authentication

CHALLENGES

- Variations among operating systems
- Extensive hardware variations and versions
- Concerns of device access and ownership

SNG POLL

HAVE YOU SEEN THE INCREASED BUZZ ABOUT TOUCHLESS/ FRICTIONLESS ACCESS CONTROL LEAD TO DIRECT INCREASES IN THE SALES OF HARDWARE LIKE AUTOMATED DOOR OPENERS?



MEGATREND MOVEMENT

Driven into the 2021 Megatrends by the COVID-19 pandemic, this trend toward to touchless and frictionless was "touched upon" in prior Megatrends reports as a micro-trend in 2019 and again in the 2020 edition, but it decisively was recognized as a Megatrend due to the health value of touchless solutions.

TAKEAWAYS

The market for touchless solutions will see steady growth, even in the post-pandemic world

Touchless is primarily influencing the access control market.

The buzz is directly linked to increased sales, with 56% of SNG respondents saying that they are seeing either some or a strong increase in new demand for touchless solutions like automatic door openers.

Smartphones have real promise for solving some friction points in security, such as visitor management.

MEGATREND 7

FACIAL RECOGNITION

Facial recognition is a complex trend. On one hand, the technology's prowess continues to grow by leaps and bounds as processing power increases and as the impact of AI comes to fruition. It is also a touchless/frictionless solution, and as such, the pandemic's effect on adoption is promising. More and more companies are competing in the facial recognition sector, which means solutions are being steadily advanced in attempts to outpace competitors. Major consumer product operating systems are applying facial recognition for device/logical authentication, notably Apple's Face ID and Windows Hello. All of this is good for business and good for the long-term trend of facial recognition.

On the other hand, the technology continues to face challenges with public perception (even though public polling indicates majority support). As the technology grows in consumer applications, the industry faces public concern that the technology would be used unethically or that there are inherent biases in the technology, and competitors are working together through groups like SIA to overcome these often unfounded concerns.

PERSPECTIVES

"The Megatrends of AI and facial recognition technology come with some serious ethical concerns that we need to be ready to deal with as good corporate citizens."

– *Grady Crosby, Chief Diversity Officer, Vice President of Public Affairs, Johnson Controls*

"The one thing that could help accelerate adoption of facial recognition would be having a clear legal framework in the public domain."

– *Richard Carriere, Senior Vice President and General Manager, CyberLink*

STATS

Research firm Markets and Markets noted that the global facial recognition market is projected to grow to $7.0B USD by 2024, up from $3.2B in 2019. This reflects a forecasted CAGR of 16.6%.

AI IMPACT

Technology advances in facial recognition are being driven by AI processing improvements. One-to-one facial matching may be the norm today, but increased computing power and AI could mean more ability to deploy facial recognition in crowded environments on moving subjects in real time.

CHALLENGES

While anti-FR groups have mobilized campaigns, SIA and members have responded with efforts to share the positive aspects of facial recognition and to clarify and explain the meaning behind often-misunderstood research. SIA has also released an extensive guide to ethical principals for use of facial recognition.

MEGATREND MOVEMENT

Facial recognition launched itself into the #3 trend spot in our 2020 report, and fell to #7 for 2021, but there are indicators that this trend is bound to stay hot for many years in the security industry, particularly since facial recognition is applicable to both access control and video surveillance.

RELATED TRENDS

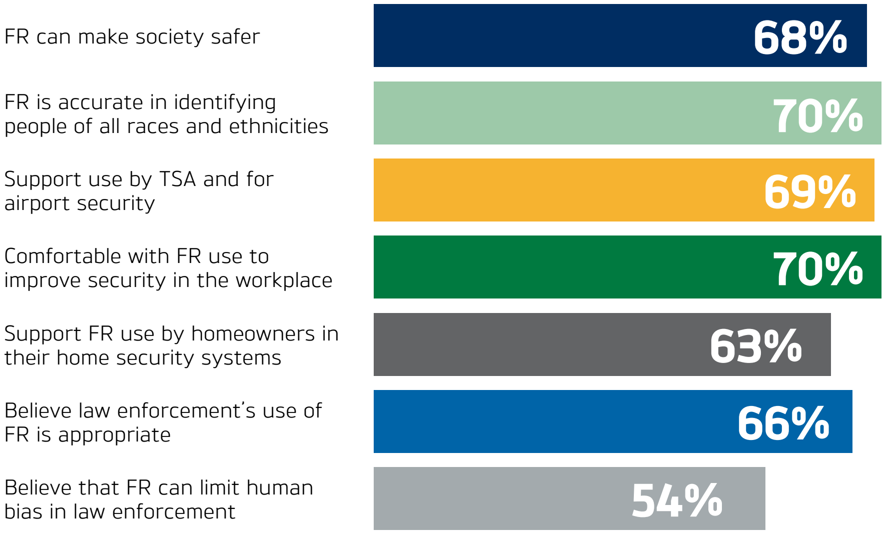
1 AI

6 TOUCHLESS & FRICTIONLESS SOLUTIONS

9 EMPHASIS ON DATA PRIVACY

STRONG PUBLIC SUPPORT

In a survey of U.S. adults from August 2020, Schoen Cooperman Research found widespread public support of facial recognition applications:



TAKEAWAYS

Studies like NIST's report, "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects," have shown that facial recognition technology performs far more effectively across racial and other demographic groups than widely reported, but the industry must still seek to eliminate any possible bias in technologies.

Localized facial recognition bans continue to be a problem for the industry.

Public opinion of facial recognition is generally positive.

Technology continues to improve dramatically, and AI advancements will continue to create more opportunities in facial recognition.

MEGATREND 8

RESPONSIVE ENVIRONMENTS & INTELLIGENT SPACES

From smart cities that can use security cameras to provide extra value like alerting on illegal dumping to commercial facilities that adapt energy usage based on facility access control, this Megatrend holds the promise of applying rules and intelligence to automate and improve environments for human inhabitants, be that through security or comfort and efficiency.

Often defined by the specific environment – smart home, smart building, smart city – the future promises that AI will process the data of an extensive sensor network and even autonomously correlate inputs and data and then develop the rules that would make the environment "intelligent." The security industry stands to be well positioned in this future thanks to its experience developing, deploying and integrating sensor solutions that can detect and control entry, motion, video, thermal and audio.

PERSPECTIVES

"We're seeing new rules related to workforce automation – driven by rules and interconnected systems. Companies are using security solutions for automated workforce management."

– Stephanie Mayes, Vice President of Sales, Americas, Synectics

"The IoT is therefore a fundamental enabler of smart environment, such as smart homes, smart health, smart cities and smart factories, among others. Indeed, the trend towards smart-x promises a revolution for most kinds of human-related activities."

– "Internet of Things for enabling smart environments: A technology-centric perspective," Journal of Ambient Intelligence and Smart Environments, January 2019

AT HOME

Homes has seen steady adoption of smart technologies, and although in August 2020, ABI Research predicted a slow-down in smart home growth due to the economic impact of the COVID-19 pandemic, the home still has great promise for accelerated impact of this trend due to the number of tech devices in homes (voice assistants, security systems, lighting automation, HVAC controls) and thanks to the more controlled environment of a home with few residents versus an office building or industrial setting.

AT WORK

Work environments are much more complicated than the home. They bring the challenge of more square footage, more mechanical and control systems, often greater security requirements, more human inhabitants and specialized uses of different spaces. However, while requiring more effort to automate and make responsive than a home, the business use case has greater financial impact, via improving worker productivity or controlling the large energy costs of a business.

IMMEDIATE APPLICATIONS

- Lights automatically turn on with arrival of users/residents
- Automatically alarming home or facility when residents/workers are not present
- Carbon monoxide sensor in garage triggers garage door to open
- Automatic leak detection and water shutoff
- HVAC automation based on occupancy or even predictive schedules

THE BUZZ

Today, most automation scenarios are manually programmed, but according to ADT's Don Young speaking at SNG 2020, the future incorporates "ambient computing" which applies AI and machine learning to recognize user needs and habits and then generate the relevant automation rules for the individual.

STATS

36%

Portion of smart home market that is predicted to come from North America

Source: Technavio, June 2020

22.6%

Portion of smart home market represented by monitoring and security solutions in 2023

Source: IDC

MEGATREND MOVEMENT

With so many important trends, this trend did not rank in the top 10 on the 2021 SECURITY Megatrends list but was recorded in the 2019 report as "Security Integrated in Smart Environments." The ranking of this trend again is likely tied to the impact of AI being the #1 tend for 2021, as AI promises to unlock real changes in smart homes, buildings and cities.

TAKEAWAYS

Today's responsive/smart environments are using rules that must be manually programmed, but tomorrow's smart environments will actually recognize needs automatically and build the rules to support those needs.

This trend is clearly tied to security, but also convenience, comfort, efficiency and (in the work environment) productivity.

Security is a core element of any smart environment.

MEGATREND 9

DATA PRIVACY

Owing much to the institution of the European Union's General Data Protection Regulation in May 2018 and the California Consumer Privacy Act of June 2018, data privacy has shaped all businesses, and certainly has driven change in the security industry, which has the potential to collect a high amount of personally identifiable information on individuals of all types due to the nature of the always-monitoring solutions.

Data privacy clearly shapes programs like background screening, but data privacy also factors heavily into biometrics, access control and general application of video surveillance. As a trend, it is closely related to the adoption of cloud services and cybersecurity, as data privacy should influence cloud implementation policies and breaches could lead to data privacy losses.

PERSPECTIVES

"Specifically in the United States, data privacy legislation has become a top priority at the local, state, and national level. New legislation proposals are being presented at increasing rates because of the pandemic work-from-home environment and the increased data exposure citizens face working outside traditional facilities. Security professionals will need to adopt to these new laws and governances around data privacy by being more sensitive to how data is collected and used, as well as how consent factors into the environment in which they are operating. It is important to be able to offer end users options, such as differential privacy technology as with privacy masking or redaction, to secure and protect the personally identifiable information (PII) of the data subjects it collects."

– Antoinette King, Key Account Manager, Axis Communications

"One thing that we have seen is an increased focus on privacy concerns as you start talking about facial recognition analytics."

– Jason Oakley, President and CEO, North American Video

"Data privacy is first and foremost on all of our minds. We're looking to adopt a set of industry-wide best practices that are customer centric and which drive transparency. We are developing programs focused on privacy, ethics and transparency and working with partners – dealers and other industry organizations – to enhance privacy and ethical standards. So we're all in on data privacy."

– Donald Young, CIO and EVP Field Operations, ADT

ACCESS CONTROL FOR CONTACT TRACING

Asked if there is an opportunity to use access control for contact tracing, LenelS2's CTO Ewa Pigna said at SNG 2020: "Yes, definitely. From a technical standpoint, it is absolutely possible. I think the area here to be concerned with is obviously data privacy and so this has to be in line with HIPAA regulations as well as an opt-in program. And a lot of it is probably dependent on the individual's willingness to participate in automatic contact tracing."

TRUST AND CONTROL

81%

Americans who feel they have little or no control over the data companies collect about them

84%

Americans who feel they have little or no control over the data the government collects about them

Source: Pew Research Center

STAT

6 MONTHS

Average length of time before a company detects a data breach

Source: ZD Net

CUSTOMER DATA

In January 2020, in its "State of Cybersecurity Report 2020," Accenture wrote critically of businesses as a whole, saying "Security investments are failing," and reporting a statistic that 44% of organizations in their study had more than 500,000 customer records exposed in the last year.

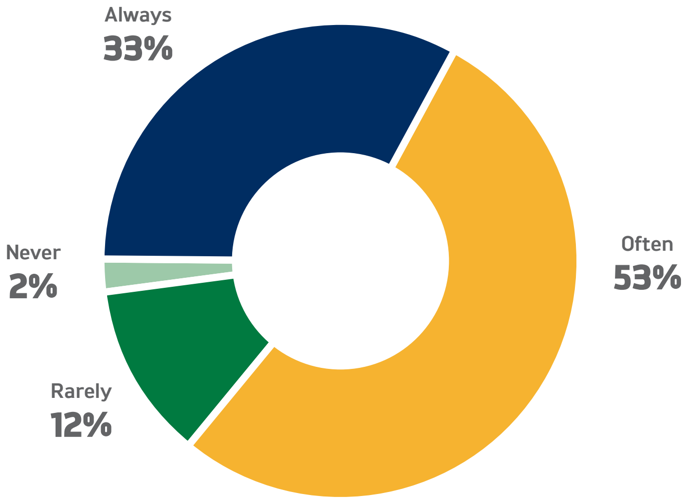
POLICY IMPACT

The California Consumer Privacy Act's so-called version 2.0 passed in November 2020 and will be implemented in 2023. It makes data privacy regulations even more strict in the state.

SNG POLL

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

The 2020 survey data indicates positive movement in awareness around data privacy, with 2% more "always" and "often" responses each, and 4% fewer "rarely" responses. The never responses stayed low, at just under 2%.



MEGATREND MOVEMENT

First ranked at #6 in 2019, then #4 in 2020, the Emphasis on Data Privacy fell to #9 in this year's report, but there are clear indications that even if it may not be the hot new trend in the industry, it is becoming a permanent fixture of conversations.

TAKEAWAYS

Security industry continues to expand its focus on data privacy.

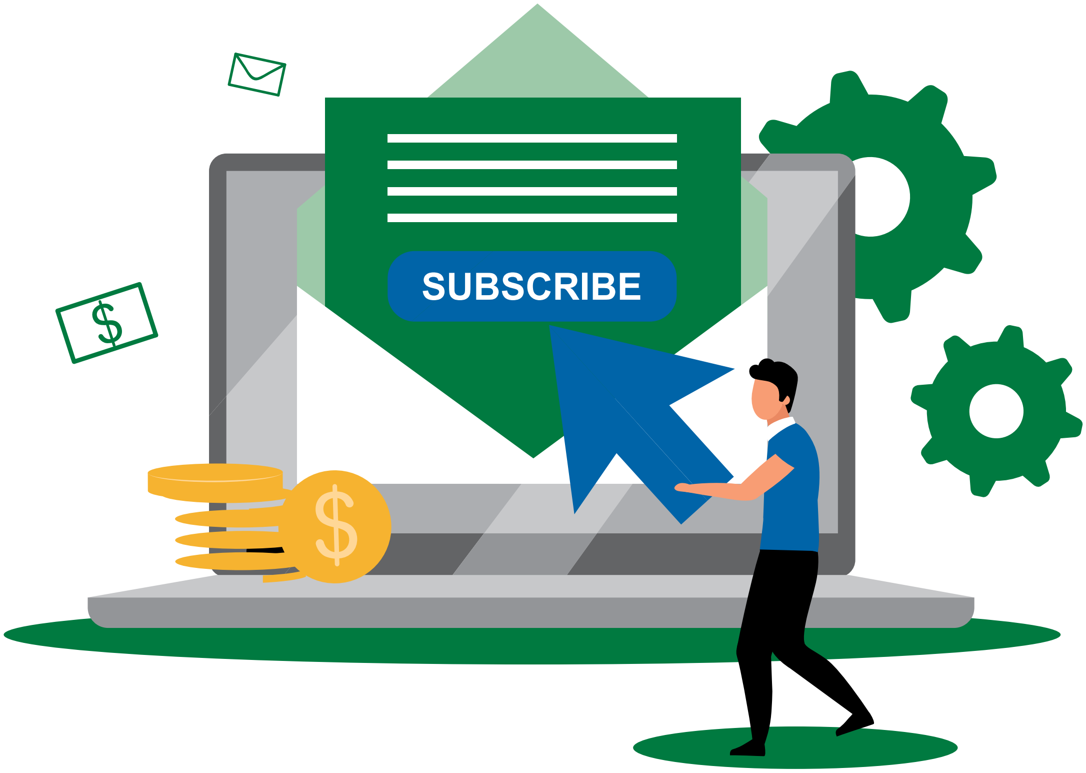
Cybersecurity breaches continue to put data privacy at risk.

Regulations continue to tighten in the U.S.

New solutions like contact tracing and facial recognition put even more emphasis on the need to have strong data privacy policies in place.

MEGATREND 10

MOVE TO SERVICE MODELS



Recurring revenue business models, or what we have called the "move to service models" trend, has been a rallying cry since our first Security Megatrends report in 2017, and the fact that it is still part of the Megatrends in our fifth report is testament to the importance of this trend to the bottom line of so many companies in the global security industry.

Although we first defined the trends as "Transformation of Systems Integrators" in the 2017 report, owing chiefly to the transformation from project-based business models to the addition of service and maintenance agreements, today we recognize that it applies to many businesses. No longer do integrators just sell the project labor and manufacturers just sell the product; today, both camps are selling recurring access to their services.

PERSPECTIVES

"Recurring revenue is very important for the software industry and will become much more important for our security industry."

– Tanja Rueckert, CEO and President, Bosch Building Technologies

"The movement to more managed services and SaaS-based business models across these different sectors is having an impact on increasing valuations."

– John Mack III, Executive Vice President, Imperial Capital

"To do it right, an integrator has to include it [an RMR-based service contract] in every quote and with every software install."

– Stephanie Mayes, Vice President of Sales, Synectics

PERSPECTIVES

“We look at things like managed services and cloud-based products, and at a time when integrators were forced to slow down a little, they have an opportunity to look at different business models and say this is the opportunity and the right environment for us to move some of our business to cloud-based models where we can look at predictive recurring monthly revenue.”

– Ric McCullough, President, PSA Security Network

“COVID has shown that companies had good RMR foundations were able to survive, because that was the predictable money. Project money has higher revenue and instantaneous impact, but RMR is what keeps the business running. The "as-a-service" model is what keeps their payroll going.”

– Nigel Waterton, Chief Revenue Officer, Arcules

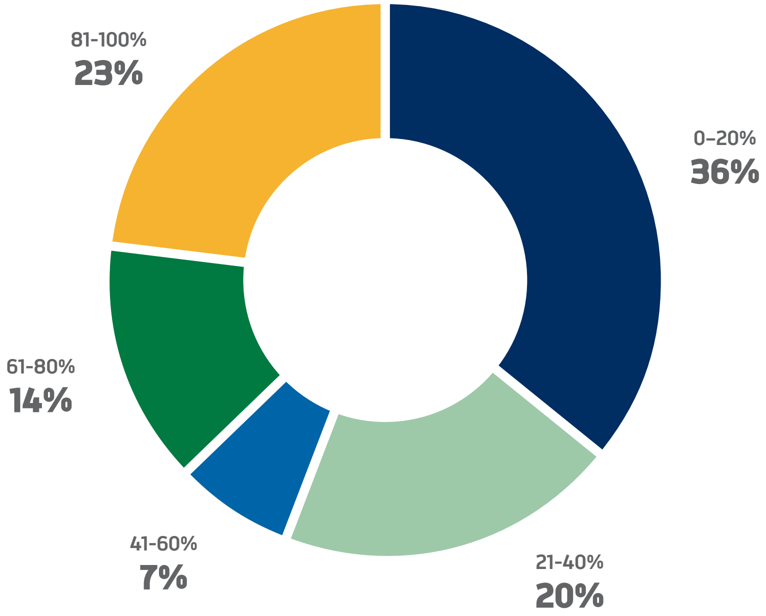
RELATED TREND

5

On the manufacturing side, this trend is aligned with the move to cloud solutions, as these are typically sold on monthly or annual “as a service” contracts, and integrators are often rewarded with a portion of that recurring income.

SNG POLL

WHAT PERCENTAGE OF YOUR FIRM'S TOTAL REVENUE IS FROM RECURRING REVENUE?



MEGATREND MOVEMENT

Ranked #5 in 2017 and 2018, then #7 in 2019, #9 in 2020 and now ranked #10 in the 2021 report, this trend is poised to fall off the ranking in next year’s report. Today there is general consensus that recurring revenue models – or service models – are now just part of life and business, much like consumers no longer buy entertainment content like movies and music, but purchase access to services that deliver that content.

TAKEAWAYS

Investors and acquirers are giving higher valuations to companies with more recurring revenue.

Growth of cloud services connects directly to the growth of “as-a-service” business models.

Most security businesses have incorporated some form of recurring revenue into their income streams, even if it is not yet the largest portion of the company’s gross revenues.

COVID-19:
THE DISRUPTOR THAT MATTERS

SIMULTANEOUSLY CREATING RISK AND OPPORTUNITIES FOR THE SECURITY INDUSTRY

THE PANDEMIC'S EFFECT ON THE SECURITY INDUSTRY CANNOT BE OVERSTATED, and that disruption was not just limited to 2020. To borrow a term that became so synonymous with the pandemic, the "new normal" for the security industry has brought exceptional new opportunities along with the negative impacts that businesses felt.

First, the bad news. A Q3 2020 Omdia report produced exclusively for SIA and studying the economic impact of the pandemic forecasted a 4.6% decline in security spending for North America in 2020 before a slow recovery in 2021 that could bring spending back to the 2019 levels. As a result, financial experts have predicted a cut in private equity investment volume in all businesses, including the security industry, although that also has not occurred as of this writing.

EDITOR'S NOTE: In a normal year, we identify a small number of disruption points that could impact the security industry. For the 2021 report, it was clear that the key disruption was and is the COVID-19 pandemic.

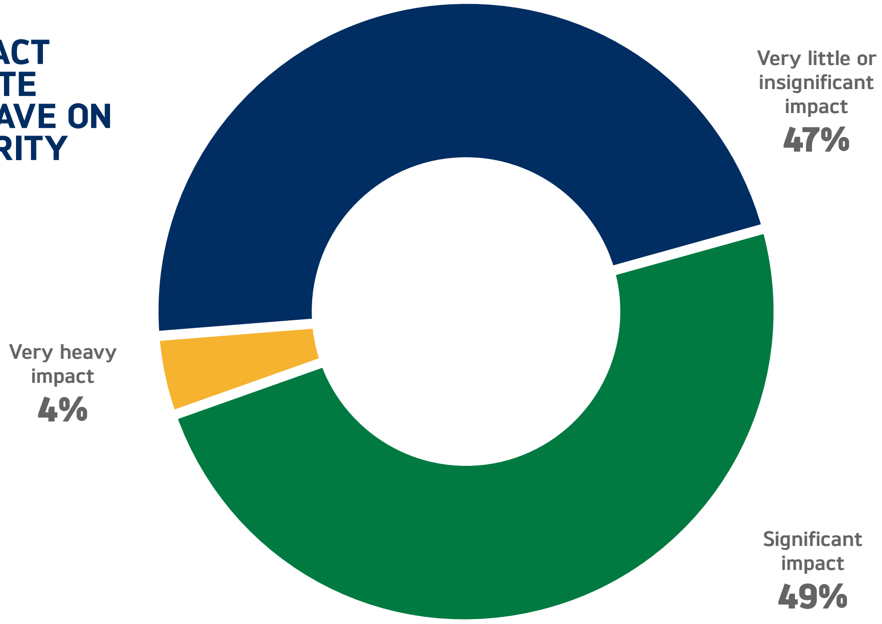
The pandemic has sent many office workers home and this work-from-home trend raises deep questions about what that will mean for security spending. While some organizations have taken advantage of the downturn and absence of employees to make security and facility upgrades, some security industry businesses have reported fewer projects in their sales pipelines.

In fact, most security industry business leaders, when surveyed during the 2020 Securing New Ground conference, said that they expect negative impact on security spending at offices. Some 54% said the impact would be "significant" or "very heavy" due to the trend of remote work.

In the survey, however, nearly half of business leaders responding said the impact of remote work was likely to have very little or insignificant impact on security spending, which brings us to the good news.

SNG POLL

HOW MUCH IMPACT WILL THE REMOTE WORK TREND HAVE ON IN-OFFICE SECURITY SPENDING?



AN INDUSTRY RESPONDING SWIFTLY TO DISRUPTION

The COVID-19 pandemic has been a business disruptor and disruptions always create opportunities. In the security industry, innovative technology companies responded to the pandemic with new technology solutions.

Thermal temperature screening solutions were introduced. Video analytics providers developed mask-detection algorithms. Facial recognition providers worked quickly to ensure matching could still function with a portion of the face obscured. Access control providers used data from their systems to help businesses study and monitor facility usage; these data points could also be used to support social distancing and return-to-work plans.

Security solution vendors with cloud capabilities found the remote access and management welcomed by practitioners. Companies that produced touchless solutions like ADA-compliant type door openers or optical turnstiles and other such hands-free devices generally reported positive financial results.

The pandemic has also strongly increased the valuations of cybersecurity companies as business leaders see even greater importance in cybersecurity investments when workers are mobile and when customer and client data is now literally in the homes of employees.

As the dominant disruptor, the impact could be permanent. Even once a vaccine is widely available, many in the industry say that they do not expect a total return to old norms, but an adoption of many of these new norms. That lasting response is not surprising, and the industry shows all indications of not only adapting to this disruption but growing and innovating because of it.

SIA
SECURITY INDUSTRY ASSOCIATION

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