2023 SECURITY MEGATRENDS™

THE ANNUAL VISION FOR THE SECURITY INDUSTRY

SIA
SECURITY INDUSTRY ASSOCIATION

MEGATRENDS TEAM

DON ERICKSON
SIA CEO
derickson@securityindustry.org

GEOFF KOHL
SIA Senior Director of Marketing
Author, 2023 SECURITY MEGATRENDS Report
gkohl@securityindustry.org

KEVIN MURPHY
SIA Director of Member Services
kmurphy@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

2023 SECURITY
MEGATRENDS™

The Insatiable Creativity of Problem Solvers

One of the things I love about our industry and SIA members is the implicit creativity. They say that "nature abhors a vacuum," and I would say that the same could be said of our industry, which grinds away to always deliver new offerings (like autonomous devices, megatrend #9) or push the limits of technology (as with artificial intelligence, trend #2).

This creativity is, in large part, driven by the entrepreneurial nature of our industry. The importance of staying one step ahead of attackers and nefarious actors is the ultimate motivation for such an unyielding desire to innovate and protect people and property.

With that, it's not surprising in the least to see the cybersecurity of physical security reign again in our list of 2023 Security Megatrends. In October, a Gartner survey of CIOs found that their number one focus on investment for 2023 is likewise cybersecurity – not application modernization, artificial intelligence or cloud computing. Given the geopolitical climate and the critical value that security solutions provide, it's extremely important that our industry continue to invest strongly in cybersecurity, both by hiring often-hard-to-find cyber talent (see workforce development, megatrend #3) and by testing and re-testing solutions and submitting them to the rigor of penetration testers and bug bounties. On that note, SIA is proud of the work of our Cybersecurity Advisory Board, which has produced guidelines and content that all SIA members can use for this cause.

Lastly, I'd like to address two trends that are not included in our report but which deserve mention.

Security as Proptech, a 2022 security megatrend, is not included for 2023, but we nonetheless believe there is a long-term change happening not only in proptech, but in all of security, such that the insights captured by security technology will drive not only protection of a business but the efficient operations and even growth of the business that adopts such technology.

It's also worth noting that sustainability, whether you roll it up into the larger ESG trend or narrowly define it as a push to decarbonization, is not on the 2023 list. Nonetheless, we do want to emphasize the importance of sustainability in our industry. Many of our SIA members rightfully study and attempt to minimize their corporate environmental footprint, but this trend is also about the way our industry's services and solutions can be used to make the world more efficient in a smart buildings type of approach. So, while not included, it is nonetheless a defining trend for us here at SIA and something important to our future as humans, especially now that there are an estimate 8 billion of us on the planet. At SIA we're also making a commitment to ESG by forming an ESG Advisory Board which will provide content and recommended practices that will be most helpful to mid and small businesses in particular. The ESG Advisory Board will begin its work in January.

To our members: Thank you for your input in shaping these megatrends and then allowing us to share them as the 2023 Security Megatrends. These are the trends that are impacting not only our industry, but we believe that are also touching the broader tech industry and the world at large.

Sincerely,

James Rothstein
Chair, SIA Board of Directors

SECURITY INDUSTRY ASSOCIATION

SNG™
SECURING NEW GROUND

THANK YOU

SIA THANKS ITS 2023 SNG SPONSORS

ASSA ABLOY

ALLEGION

AMAG TECHNOLOGY
An ALLIED UNIVERSAL® Company

AXIS COMMUNICATIONS

AXON

BOSCH
Invented for life

brivo
simply better security

cloudastructure

convergint

dormakaba

EAGLE EYE NETWORKS

Hanwha Techwin America

Houlihan Lokey

Imperial Capital

LENEL·S2

LOUROE ELECTRONICS

milestone

MOTOROLA SOLUTIONS

PROSEGUR SECURITY

PSA SECURITY NETWORK

RAYMOND JAMES®

System Surveyor

UNLIMITED TECHNOLOGY

wesco

PREMIER SPONSOR OF

ISC

MEDIA SPONSORS

SDM

SJA SECURITY JOURNAL AMERICAS

SNG™

SECURINGNEWGROUND®

THE BUSINESS OF SECURITY

SAVE THE DATE

OCTOBER 17 – 18, 2023 | NYC

SIA
SECURITY INDUSTRY ASSOCIATION

HOW WE DEFINED AND RESEARCHED THE 2023 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 ideas are shared openly.

In advance of SNG, as part of our annual membership survey, SIA asked hundreds of executives from SIA member companies what factors were shaping their business decisions and what trends they were watching. We then further surveyed SIA members, along with current and recent speakers and attendees of SNG about which previous trends were still relevant, which trends were no longer as impactful to the industry and which trends could be identified to be added to our report.

In the fall of 2022, a group of SIA Megatrends advisors, Steve Van Till of Brivo, Brian Ruttenbur of Imperial Capital and Tara Dunning of Wesco, provided focused feedback on the megatrends via in-depth conversations. The value of insights from these leaders and luminaries cannot be overstated (thank you, Steve, Brian and Tara!). SIA simultaneously gathered feedback from the SIA Executive Advisory Board (chaired by Tom Cook of Hanwha Techwin America), and we are indebted to the critical input and wide-ranging perspectives this group shared.

In addition to the survey research and the focused conversations, the selection of these trends relies on the speakers, panel and audience members of SNG, because the conference is the ultimate proving ground for deep-dive discussions on what we can do as an industry to pave a successful future. A special poll-driven session during the 2022 SNG conference (hosted by Van Till and Ruttenbur) provided additional feedback related to the Security Megatrends and helped generate some of the chart data included in this report.

Lastly, as we authored this report, we tried to reflect not only the vendor/integrator/service provider side of the industry but did something we had never included before—which was to reflect each trend's impact on the security practitioner or CSO.

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 2023 SIA Security Megatrends report, but also provided you insights and action items to facilitate a successful future in the security industry.

Geoff Kohl
Editor, 2023 Security Megatrends report
Sr. Director of Marketing, SIA

2023 SECURITY MEGATRENDS

MEGATREND 1

CYBERSECURITY OF PHYSICAL SECURITY

MEGATREND MOVEMENT

AI and Cybersecurity continue to jostle for the top trends impacting the security industry, but the data was clear: Cybersecurity is top of mind for security industry leaders.

As a top megatrend that has always ranked #1 or #2 since we first published the Security Megatrends research in our 2017 edition, the ranking at the top of this list underscores the fact that security has truly converged, whether we think it has or not.

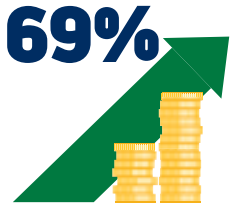
Now that the security industry has made nearly every sensor, system, software and server/recorder and device interconnected and remotely available, the question that buyers ask is not just, "How does this help protect my people, assets and information?" but is, "While you promise to improve my security, what cybersecurity risks does your system create for me?" Today, federal government buyers require specialized cybersecurity assurance and certification from vendors and contractors, and end users are closely watching industry news reports and sharing information on weaknesses and strengths of security industry service providers and vendors—and their cybersecurity mistakes. The convergence was underscored in 2018 when the Department of Homeland Security created the Cybersecurity & Infrastructure Security Agency, a group whose mission is to engage the private sector specifically on converged threats to core U.S. infrastructure. But the convergence has been challenging on vendors, integrators and practitioners as their scope of work and duties has expanded greatly (see Business Impact section).

BUSINESS IMPACT

Many large buyers now provide a cybersecurity questionnaire that integrators and solution vendors must complete, leading to creation of new roles in some companies just to respond to such questionnaires that are required in bid processes. Vendors, integrators and the practitioners themselves are simultaneously chasing cybersecurity talent to add to their employee teams, a challenging proposition given the overall difficulty to hire technically skilled workers of any type.

Cybersecurity has to be managed on multiple levels, requiring constantly expanding investments in:

- Device-level cybersecurity (e.g., cameras, readers, panels)
- Infrastructure cybersecurity (wiring, networks, switches, etc.)
- Software and Server cybersecurity
- Configuration cybersecurity (correct implementation of cybersecurity features)
- Cloud cybersecurity
- Mobile device cybersecurity (particularly as security and employee bases become more mobile or remote)
- User cybersecurity (e.g., social engineering attacks, insider threats, etc.)



Businesses that planned to increase their cybersecurity expenditures
–TechTarget's Enterprise Strategy Group, March 2022

Average cost of a data breach
–IBM's Cost of Data Breaches Report 2022

IMPACT TO THE PRACTITIONER/CSO

In the world of the practitioner, cybersecurity is essential, and it's simply one more plane of threats from which security leaders have to contend. For the practitioner, this is also represented in a world of steadily converging security. While some top global companies today have truly converged the formerly differentiated world of physical security and cybersecurity, most still reside in a dual reporting structure but have built in regular check-ins and procedures that respect each team's expertise, while providing the benefit of eliminating the communication boundaries between the groups.

Security practitioners today seem to have three general choices when it comes to convergence:

1. **Ignore:** Disregard the need to converge—a wholly unwise choice, by most accounts.
2. **Strongly Interrelated Teams:** Continue to manage security in two, separate but equal channels, but strongly define team relationships such that constant open dialogue and cross-investigation exist between the two specialized teams.
2. **Fully Converged:** Fully merge security leadership and tactical security management to link cybersecurity protections and physical security protections, given converged threat vectors that impact information, data, people and assets.

SNG POLL

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

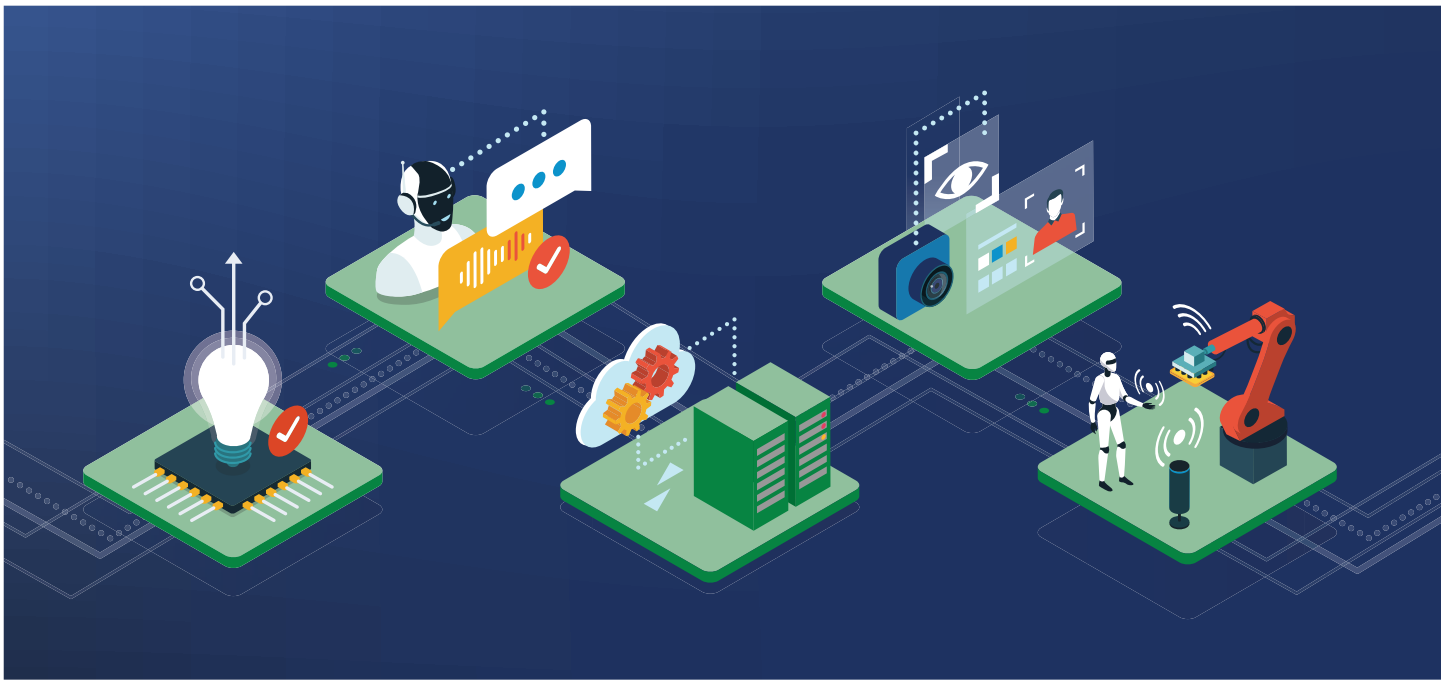
When we first asked this benchmark-level question for our 2020 report, over 8% of respondents surveyed at SNG indicated that cybersecurity was rarely a discussion point. That number has steadily fallen, and today only 3% report that cybersecurity is rarely a question engaged with security practitioners. We can presume (or at least hope) that those 3% are selling purely mechanical, non-IoT solutions, given the constant engagement on the battlefield of cybersecurity.

DATA POISONING

Bridging megatrend #1 (cybersecurity), megatrend #2 (artificial intelligence) and megatrend #5 (ethical/safe use of data and technology) is the emergence of data poisoning attacks. Such attacks recognize that AI systems rely on complex data sets for training and learning, and that by poisoning the data pool itself with erroneous data, they can defeat the AI.

MEGATREND 2

ARTIFICIAL INTELLIGENCE



MEGATREND MOVEMENT

Falling from the #1 position in our 2022 report, AI nonetheless remains a defining trend, and AI and cybersecurity were orders of magnitude higher rated than the subsequent trends. We suspect the decrease in position is largely due to realizations that the fruitions of AI are more of an evolutionary change to the industry than an overnight change.

Dropping to #2 from our 2022 report, artificial intelligence (AI) remains top of mind for solution developers, practitioners, service providers and integrators—but it's all about the actionable intelligence that can be gained from AI. Buyers and CSOs interviewed by SIA report that they are seeking new systems, but are seeking meaningful insights that can be gleaned from their existing systems and investments. This has given rise to a field of solutions that add AI to existing camera systems, cloud and software-based systems that are add-ins to existing intrusion and access systems to help separate meaningful signals from the noise that comes with so many data points being fed to the practitioner.

Moreover AI applications on top of security solutions helps break the boundaries of our industry's value to practitioners (see trend 6, Elimination of Industry's Boundaries), by embedding non-security applications that take data from the proliferation of sensors of all types (see trend 10) to correlate data points or find trends that can save businesses money or enable them to act more swiftly.

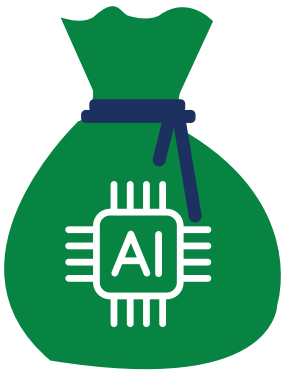
REGULATION AHEAD

Those tracking regulations, including SIA's own government relations team, forecast changes ahead for AI. While some legislative action has been to encourage and enable businesses to develop next-generation AI technology, there are also regulations (such as those on facial recognition) that have slowed down adoption. Fortunately, in the area of facial recognition, wholesale bans on facial recognition appear to be losing momentum or are being reversed as in the state of Virginia and the city of New Orleans.

In a pre-event discussion with panelists from an AI panel held at SNG 2022, the expert panelists (reflecting integrators, vendors and practitioners) indicated they see sweeping AI frameworks coming, but admitted the industry is not yet prepared to define a framework for AI, noting that the technology's rate of change is likely outpacing our ability to construct implementation frameworks, particularly ethical frameworks (see also trend #5, Ethical/Safe Use of Data and Technology).

CLOSELY RELATED MEGATRENDS

5. Ethical/Safe Use of Data and Technology
6. Elimination of Industry's Boundaries
9. Autonomous Devices
10. Proliferation of Sensors



$500B

Forecasted 2023 global spend on AI by businesses and government

Source: IDC Research

IMPACT TO THE SECURITY PRACTITIONER/CSO

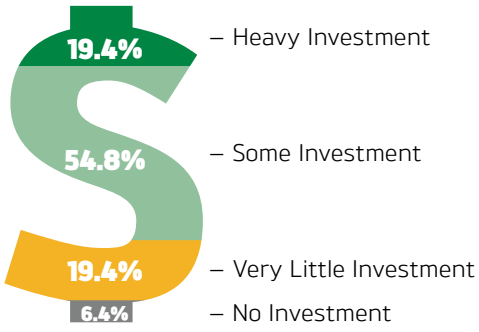
As one respondent wrote to SIA during our research collection phase of this report, the opportunity of AI for practitioners is in "risk adaptive systems." "Based on threats, systems should be able to change the security posture dynamically," wrote the respondent. "For example, based on a threat score, the readers would change modes. Many other procedures could be automatically initiated." Ultimately, that seems to be opportunity for practitioners: AI is a way to make their people and systems able to respond more effectively and to find hidden meaning in the sometimes-overwhelming amount of data that is collected by security, be that technology systems or guard staff.

PERSPECTIVE

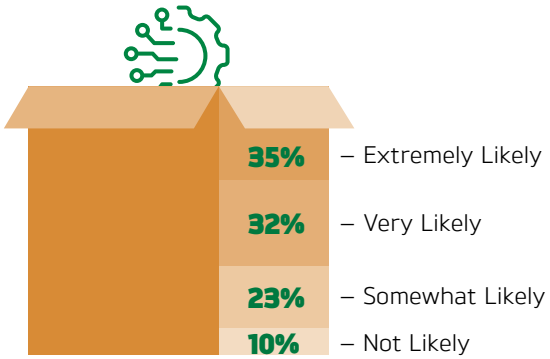
"IN 2023, ARTIFICIAL INTELLIGENCE WILL BECOME REAL IN ORGANIZATIONS. NO-CODE AI, WITH ITS EASY DRAG-AND-DROP INTERFACES, WILL ENABLE ANY BUSINESS TO LEVERAGE ITS POWER TO CREATE MORE INTELLIGENT PRODUCTS AND SERVICES."

—TRENDS FUTURIST BERNARD MARR, WRITING FOR FORBES IN NOVEMBER 2022

SNG POLL



– Heavy Investment
– Some Investment
– Very Little Investment
– No Investment



– Extremely Likely
– Very Likely
– Somewhat Likely
– Not Likely

BENCHMARK: HOW WOULD YOU CHARACTERIZE YOUR FIRM R&D INVESTMENTS RELATED TO APPLYING AI TO YOUR PRODUCTS AND SOLUTIONS?

Over time, SIA manufacturer members surveyed at SNG have reported increasing investment in AI. Today the number of companies that are reporting no AI investments is down to approximately 6%, and approximately 3/4ths of respondents indicate some investment or heavy investment.

WILL AI BECOME A MEANINGFUL FEATURE WITHIN YOUR PRODUCTS, SOFTWARE OR SOLUTIONS WITHIN THE NEXT 2 YEARS?

Predictive analytics continue to be forecast as a product development opportunity according to most manufacturers responding to a poll at the October 2022 SNG conference, with over 2/3rds forecasting such functionality as being very or extremely likely to be part of their product solutions within the next two years.

MEGATREND 3

WORKFORCE DEVELOPMENT

MEGATREND MOVEMENT

Workforce development and attracting skilled talent have continued to rise in its importance to the industry, jumping to #3 from its ranking at #5 in 2022's report.

This guide was developed as a free resource for students and others seeking to enter the security industry, and provides insights into career growth opportunities.

In the words of one 2023 Security Megatrends survey respondent, attracting skilled labor is a top concern, and there's only one solution in today's hyper-competitive labor market: "We must train our own." Long established as a factor limiting companies' growth (especially that of the systems integrators), expanding the workforce has become a key focus of organizations like SIA, which partnered with the Electronic Security Association to cofound the Foundation for Advancing Security Talent (FAST) to drive awareness of security industry employment opportunities.

IMPACT TO THE PRACTITIONER/CSO

The practitioner community long relied on the investigative and protective talent that came with hiring employees from law enforcement and military communities, and while those skills are as in demand as ever, practitioners report that they are now finding themselves better served to hire talent with technical skillsets and then train those new employees on the security component.

Smart practitioners, particularly larger corporations with extensive security teams, are also hiring talent from their integrators and vendors in some cases, recognizing that they need internal personnel with the skillsets that they once could wholly outsource. Others are instead outsourcing or embedding integrator talent into their organization, reports John Nemerofsky, chief operating officer of SAGE Integration, who has delivered such employees to his clients as embedded staff.

WHERE TALENT IS NEEDED

The shortages are being felt in four key areas:

- Installer/technician talent
- Application/software developer talent
- Networking/IT talent
- Cybersecurity talent

35.5%

Companies remarking that talent shortages are limiting their ability to grow revenues

Source: 2022 SNG poll

MAKE A DIFFERENCE

Support the work of FAST to draw awareness of our industry's incredible employment opportunities by donating or volunteering. Learn more about the important work of FAST: advancingsecurity.org. SIA's own RISE community for young professionals and SIA's Women in Security Forum are also working to ease the talent challenge, by welcoming a more diverse talent pool and developing programs that aid in retention and professional growth of those individuals.

FAST Foundation for Advancing Security Talent

Our Goal: To Help Connect Talented and Motivated Individuals With Opportunities in the Field of Security Technology and Life Safety

The Foundation for Advancing Security Talent (FAST) is dedicated to connecting passionate, innovative professionals with new opportunities in the electronic security and life safety industry. Through a partnership of the industry's leading associations, the Electronic Security Association (ESA) and the Security Industry Association (SIA), FAST brings awareness to the career advancement opportunities within the fast-paced technology industry that serves to keep people, places and property safe.

Support the Future of the Security Industry. Make a donation to FAST

SCAN TO DONATE

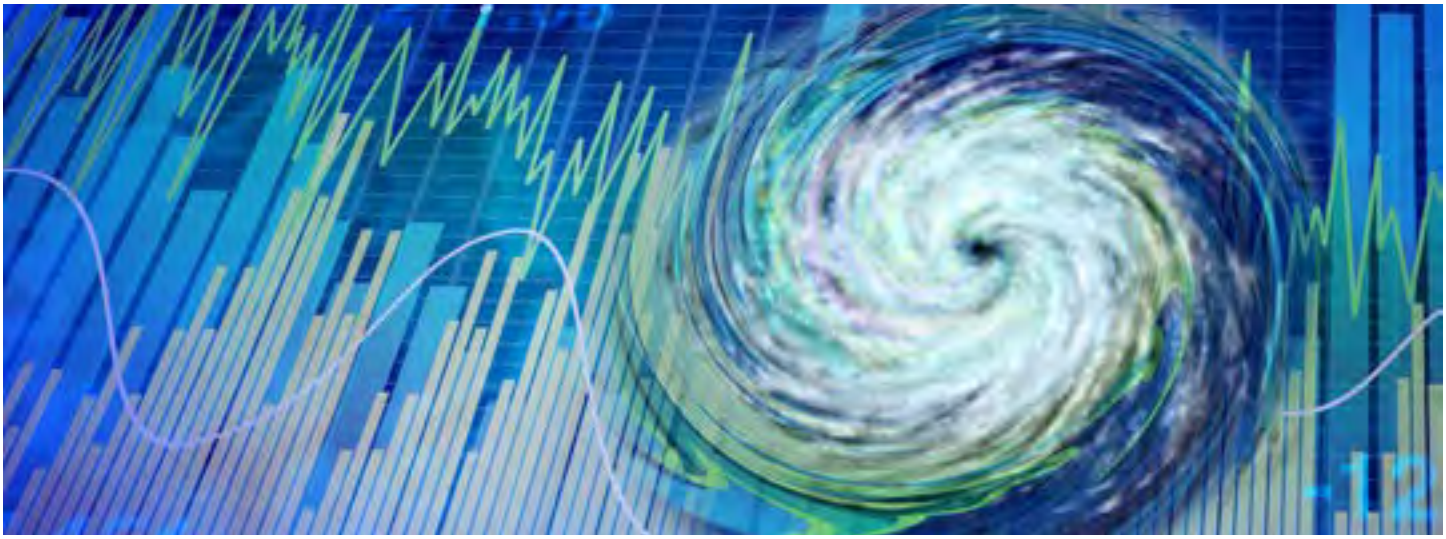
Your Gift Supports

- Student outreach efforts to drive awareness of security industry opportunities
- Outreach to underrepresented communities
- Development of workforce training programs
- Research and resources to help your company attract and retain talent

advancingsecurity.org

MEGATREND 4

CHANGING ECONOMIC CONDITIONS



MEGATREND MOVEMENT

This megatrend was new to the list for 2023, coming after a decade of steady growth in the industry, but influenced by global disruptions in health, supply chains, trade and geopolitical disputes.

POSITIVES AND NEGATIVES IMPACTING THE INDUSTRY

Positives
Commercial Demand
Strong Backlogs
New Offerings
Supply Chain Pressures Easing
Negatives
Decreased Consumer Demand
Public Co. Performance
Slowing of New Hiring
Margins Haven't Fully Recovered

Source: Imperial Capital

The S&P 500 officially reached bear market status in mid-June 2022 when the market dropped 20% from its high over two consecutive quarters. Interest rates have simultaneously increased steadily with movements from the Federal Reserve Bank, and that is slowing new construction in both residential and commercial sectors. With overall inflation at around 8% (although slowing according to the U.S. Labor Department), burden is being placed on suppliers who strive to minimize cost increases to their clients, and to the clients themselves, who are finding double-digit cost percentage increases in some areas, especially in labor costs.

The impact is multi-fold. These adjustments in economic conditions have already limited the number of investments and acquisitions taking place in the market according to Imperial Capital's John Mack, Raymond James' Alper Cetingok and Egis Capital Partners' Robert Chefitz during their 2022 SNG session and has all but eliminated movements to take companies public. Construction decreases have the real opportunity to slow the pipeline of new security projects (particularly in the residential space, as the commercial space is still amid an upfit wave recognized in the 2022 megatrend of proptech). Additionally, "megatech" company layoffs in the fall of 2022 have many other companies nervously watching for cascading effects on the overall economy, although some SIA members report that they are targeting some of these skilled workers to fill open positions at their firms. The SIA Security Market Index, a bimonthly industry confidence report, put the overall confidence at 52, down from 72 in February and April (the confidence score is rated on scale of 1-100, with anything above 50 being positive).

But there are mixed signals: 70% of respondents to the October 2022 SIA Security Market Index expected conditions to be a little or much better in the next three months. And in a poll at SNG in October 2022, many reported that their pipelines for sales were stronger now than before the pandemic.

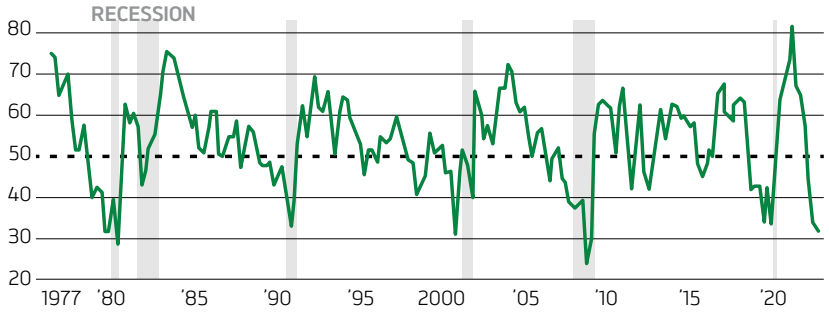
Ultimately, many careful eyes in the industry know that boom times won't last forever, and with the war in Ukraine, rising fuel costs globally (particularly in Europe), inflation in the U.S. and Europe, and trade wars with China, the ingredients are there for economic cooling.

IMPACT TO THE PRACTITIONER/CSO

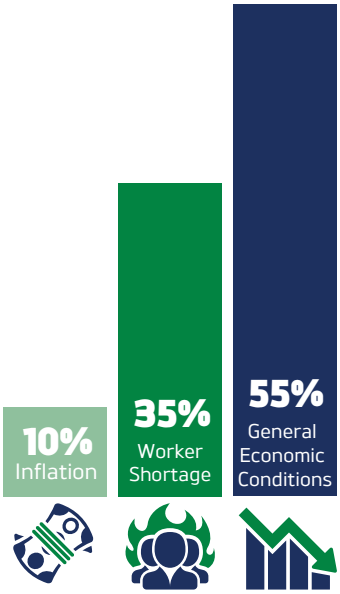
If economic conditions do worsen, security practitioners will do what they do best: Do more with less. Already in a position where they scour the field of security with an eye to how they can double-task a security solution to provide business operational value in addition to the security/safety value, they will nonetheless strive to creatively find even more opportunities to position investments in security as investments in the business itself, and not just in the protection of the business, its people and its assets.

A DROP IN CEO CONFIDENCE

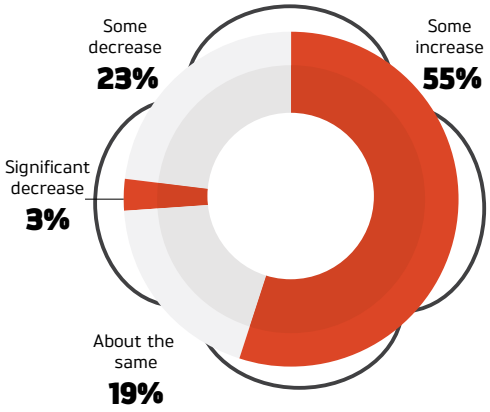
Shared by Nasdaq Chief Economist Phil Macintosh at SNG 2022 was data that CEO confidence had gone from an extreme high in late 2021 to lows not seen in over a decade.

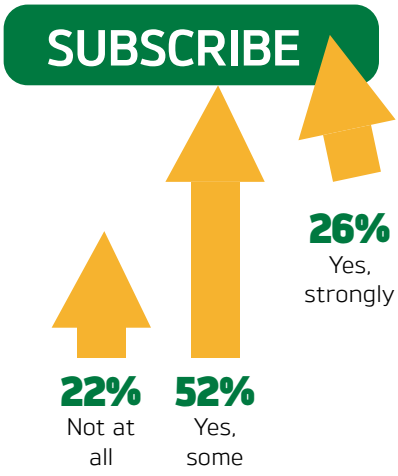


SNG POLL



Source: WSJ Conference Board





WHICH OF THE FOLLOWING FACTORS DO YOU BELIEVE WILL MOST SIGNIFICANTLY IMPACT YOUR BUSINESS GROWTH IN THE COMING YEAR?

It's the economy. Nearly 55% of SNG respondents indicated that "general economic conditions" are the top concerns likely to impact their business in 2023. More interestingly, not a single respondent selected supply chain delays, indicating that the anxiety of security industry business leaders is now focused on new areas—and once again, largely out of their control.

HOW WOULD YOU CHARACTERIZE THE RECOVERY OF YOUR PROJECT/SALES PIPELINE TODAY COMPARED TO PRE-PANDEMIC LEVELS?

SNG attendees were polled to determine how their sales/project pipeline stands today (or as of October 2022) compared to pre-pandemic levels. The good news: nearly 55% said they had experienced some increase. Just under 20% said it was about the same, and slightly over a quarter indicated some decrease or a significant decrease. None reported a strong increase.

WOULD WEAKENING ECONOMIC CONDITIONS DRIVE YOUR COMPANY TO ADOPT MORE RECURRING REVENUE/SUBSCRIPTION/ AS-A-SERVICE MODELS?

One of the conjectures of the SIA Megatrends Advisors was that challenging economic conditions would favor companies that have stronger RMR income.

MEGATREND 5

ETHICAL/SAFE USE OF DATA AND TECHNOLOGY

MEGATREND MOVEMENT

Renamed from "data privacy" megatrend in our 2022 report, this megatrend has increased in its importance to the industry. We believe its 2023 ranking as a top 5 trend is largely driven by continued awareness of data privacy concerns and customer and policy landscapes that now look at appropriate use of technology to match customers' own paradigms in social and governance factors of ESG.

"THE PRICE OF GREATNESS IS RESPONSIBILITY."

—WINSTON CHURCHILL

Churchill's message may have been for political leaders, but it's just as true in the world of security and technology, where the greatness comes in new capabilities of cutting-edge technology and in the vastness of data collected. While we previously described this trend in the narrow light of data privacy, it has become clear that the overarching trend is how to ensure that the powerful technologies (like AI-enable systems) and the data lakes we are creating are used for good.

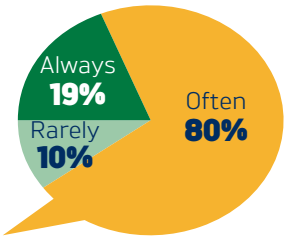
The industry as a whole has embraced this awareness, particularly with SIA creating frameworks for responsible use of facial recognition ("SIA Principles for the Responsible and Effective Use of Facial Recognition Technology") and data privacy guidelines (including the documents "SIA Privacy Code of Conduct," "Reducing Risk, Seizing Opportunity: A Security Industry Guide to Privacy" and the new "Data Privacy Code of Practice for Video Surveillance"). SIA also provide guidelines within its "SIA Member Code of Ethics."

IMPACT TO THE PRACTITIONER/CSO

Ultimately, the practitioner is responsible for ensuring that their data is protected and that systems are used ethically. This had led to pullback from many practitioners on their pace of adoption for some technologies like facial recognition to ensure that they have not only justifiable use cases but the procedures in place to ensure that advanced systems are used responsibly, and that data is only collected when it is needed.

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

In our 2022 version of this same poll, 17% reported that conversations around data privacy were rarely or never held with customers. Today, the "never" responses have been entirely eliminated, and only 9.6% report that they rarely discuss data privacy with clients. Nearly 20% report that they "always" discuss data privacy with clients, approximately the same as the 2022 data.



MEGATREND 6

ELIMINATION OF INDUSTRY'S BOUNDARIES

MEGATREND MOVEMENT

New for the 2023 Security Megatrends report, this megatrend nonetheless draws from previously reported megatrends like "Increased Interoperability" (2022 report) and the consistent megatrend of "Artificial Intelligence."

ADT expanded into solar. State Farm invested in ADT. NRG Energy announced the purchase of Vivint. Google, Amazon and other megatech players have moved into security. And it's not just limited to the residential market. Simultaneously, companies that had once marketed their services and technologies as security specific began to deliver services that contribute to operational performance—be that aspects like people counting and dwell time for retail, smart city monitoring for urban applications, tenant experience improvements in the world of proptech and building occupancy analysis in the world of commercial real estate. The concept is often referred to as the "return on security" or "return on security investment" and reflects a movement to invest in security solutions and services that enable their bottom line.

Simply put: security solutions can no longer just be for security. Whether you call it the multi-purposing of security solutions, "beyond security" or the removal of boundaries, the movement is clear: Buyers are thinking more holistically about the business impact of any equipment or technology service purchase, and businesses are more likely to get the contract if they can provide multi-purpose value.

"TRADITIONALLY SECURITY IS BEING REDEFINED BY THOSE OUTSIDE THE INDUSTRY, AND IT'S NOT CLEAR THAT THE INDUSTRY SEES WHAT IS COMING. DIY WAS ONLY THE START. WHO CAN CONTROL THE HOME WILL DEFINE WHO WINS IN THE FUTURE. WILL SECURITY BECOME JUST ONE ELEMENT OF A LARGER SYSTEM THAT WILL NOT BE CONTROLLED BY A DEALER?"

—ANONYMOUS SURVEY RESPONDENT

RELATED MEGATRENDS

- 2 Artificial Intelligence
- 4 Changing Economic Conditions
- 10 Proliferation of Sensors

A change driven by AI and sensor growth: The ability to do more with security solutions is coming from analytics and AI and the steady increase in the number of sensors at a customer's facility.

With the likelihood of changing (i.e., worsening) economic conditions, justification for security investments will require more scrutiny, thus driving more practitioners and business leaders to require multi-purposing of security solutions. As Van Till noted in his talk with Ruttenbur at SNG 2022, this ultimately has the opportunity to make our industry "sexy" to business executives as they consider technology investments.

IMPACT TO THE PRACTITIONER/CSO

This trend is truly driven by the practitioner, and not just by those in the CSO's suite. The camera that surveils the perimeter might also be used to verify facility condition. The access system that ensures the right people gain access can be used to provide reports that help verify service visits by business vendors' service technicians. Cameras once bought for loss prevention are giving retailers insights into customer activity. Some practitioners are thinking even further ahead: sell the solution internally to their company stakeholders on the operational merits of such technology and receive the security applications of these technologies as a by-product.

MEGATREND 7

SECURITY AS A SERVICE

MEGATREND MOVEMENT

Down from #4 in our 2022 report, and yet constantly discussed as the key business change in our industry, particularly for security integrators, we can only explain the drop in the rating of this megatrend as indication that as-a-service is becoming more normalized as a business model.

When we first published the first SIA Security Megatrends (the 2017 report), "Cloud Computing" was named as a trend, and even in the 2022 report, we named this trend "Service Models and the Cloud." Following extensive discussion and given general cloud adoption trends (cloud is pervasive in consumer technology and IT services and now even becoming predominant in the security industry), the discussion is no longer really about the cloud. In fact, when you hear someone say "cloud," it's often a stand-in for a service-model approach to delivering security solutions.

Today, major systems integrators are reconfiguring their businesses to not be reliant on project/install incomes. Even major manufacturers who existed in the world of building a product and selling them individually, have developed services such that they (or the channel partner) can build a recurring revenue stream. As Megatrends advisor Steve Van Till noted during the 2022 Securing New Ground conference, the recurring revenue of security as a service will prove extremely valuable for such companies during periods of economic turmoil and downturns when new installations could diminish.

"THE RECURRING MONTHLY REVENUE CONCEPT IN THE SECURITY INDUSTRY WAS ONCE DEFINED AS INTEGRATORS MONITORING AND MANAGING MONTHLY CONTRACTS WITH END USERS. WITH THE INCREASE OF CLOUD-BASED TECHNOLOGY, HOWEVER, THE RMR DEFINITION HAS EXPANDED. COMPANIES NO LONGER JUST SELL SYSTEMS; THEY ALSO PROVIDE SERVICES."

—KIM LOY, WRITING FOR SIA TECHNOLOGY INSIGHTS

IMPACT TO THE PRACTITIONER/CSO

As one government security leader told a SIA National Capital Region Security Forum during a breakfast event earlier this year, "If it's not cloud-based, I don't want it." The reasoning for such a line in the sand and a move to as-a-service solutions? He said it was because he is not in the business of managing technology systems but in the business of securing the nation and its people. His message is that he and the team he leads are more efficient at their real duties when they are not distracted by technology management, and the bonus for a mobile workforce protecting a nation from border to border is that the data and services become available, no matter whether the team member is in Washington, D.C., or in a remote area on the move. It also enables practitioners to exist in a world of continual improvement. While some as-a-service and cloud solutions still require upgrade fees, others do not charge such fees and instead build in the cost of software improvements into the monthly charges. Either way, the practitioner gains the benefit of accessing the latest and greatest features. An additional financial benefit to the practitioner is that upfront costs typically decrease when deploying a software-as-a-service solution.

BY THE NUMBERS

20.7%
projected growth of global end-user spend on public cloud services in 2023

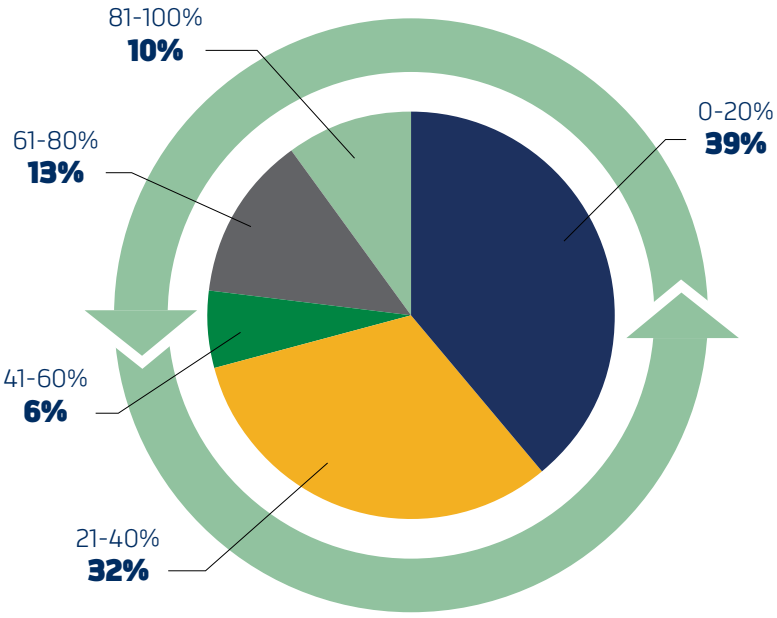
$591.8B
global total of projected spending by end users on all public cloud services in 2023

Source: Gartner

SNG POLL

WHAT PERCENTAGE OF YOUR TOTAL BUSINESS REVENUE COMES FROM RECURRING REVENUE?

Attendees of the 2022 SNG conference were asked to estimate how much of their total business revenue comes from recurring revenue. Over 2/3rds of respondents indicated that their recurring revenue was 40% or less of their overall gross revenues.



MEGATREND 8

SUPPLY CHAIN ASSURANCE

MEGATREND MOVEMENT

Dropping from a #3 megatrend ranking in 2022 to #8 on this year's list is a hopeful sign of a return to the former normal, but even being ranked at all indicates that the supply chain challenges are far from over. Business leaders like Alex Housten (dormakaba) and Mike Mansuetti (Bosch) remarked at SNG that there is unlikely a return to the former normal, and that business leaders today must more closely manage and monitor their supply chains and develop plan B, C and D type options to ensure they can deliver solutions to customers.

While speakers at SIA's 2022 Securing New Ground conference generally reported that supply chain woes are easing, the pain is still far from gone. And it's not just a challenge of getting products or getting materials. Changes in the geopolitical landscape, loss of trust in the cybersecurity of products from some trade partners, and questions about how to ensure cybersecurity chain of custody throughout the supply chain for critical components have become and will continue to be constant concerns for all in the security industry. With customers now considering other sources for product, it presents an erosion of longstanding client relationships that could once be counted upon.

TOP CONCERNS

- Raw material availability and delays
- Product availability and delays
- Cybersecurity chain of custody and trust of source components
- Loss of exclusive purchasing arrangements with longstanding customers

IMPACT TO THE PRACTITIONER/CSO

At a gathering of top CSOs in the summer of 2022, when asked about pain points, a surprising number of security practitioner leaders said that product availability of security solutions from their vendors was among their top concerns, as it was limited their ability to secure facilities, make upgrades and ultimately protect the people and assets they were tasked with protecting. Retired industry luminary Phil Aronson (formerly of ASG and ADT) noted that it was remarkable to hear the individuals comment on this concern. Practitioners attending the fall 2022 Securing New Ground conference provided similar concerns during a supply chain panel, and some indicated a lack of communication on this issue and expressed wonder if only the biggest clients were getting priority for backordered solutions. Many practitioners and their integrator partners have adapted by sourcing products from new vendors who have survived supply chain challenges more or less intact.

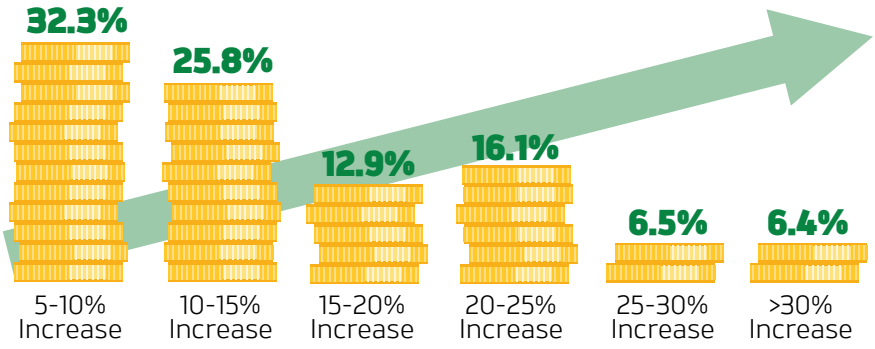
SNG POLL

WHAT LEVEL OF PAIN ARE SUPPLY CHAIN WOES STILL CAUSING YOUR BUSINESS TODAY?

The new grey hairs on the heads of industry leaders aren't just from how to protect against emerging cyber-attacks, how to attract talent or where to invest their R&D dollars in AI. They are from the supply chain woes still being experienced. 75% of SNG poll respondents indicated strong pain continues and almost 13% reported extreme levels of pain caused by supply chain issues.

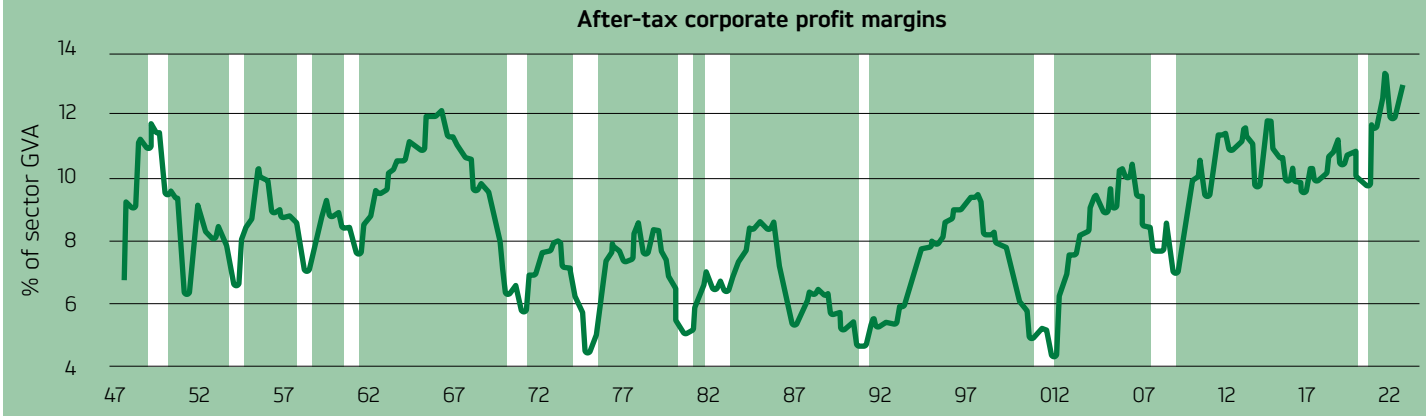
HOW MUCH ON AVERAGE HAVE THE COSTS OF THE SOLUTIONS/ PRODUCTS/SERVICES YOU PROVIDE INCREASED OVER THE LAST 12 MONTHS?

The inflation rate may be hovering around 8% across the Consumer Price Index, but the costs appear to be even more dramatic in the world of security technology services and solutions. Only a third of respondents put their price increases in line with the U.S. Labor Department's data. Approximately a quarter of respondents placed the increase at 10-15%, and a not inconsequential 6.4% put their increases at over 30% in the last 12 months.



SHORTAGES IMPACT ON MARGINS

Nasdaq Chief Economist Phil Macintosh reported at SNG 2022 that the one upside of supply chain delays is that it actually improved margins for suppliers as a whole (not just the security industry).



Source: JP Morgan, BEA

MEGATREND 9

AUTONOMOUS DEVICES/ROBOTICS

MEGATREND MOVEMENT

Autonomous Devices, which is new to the Megatrends list for 2023, has always earned a significant number of votes to put it under consideration as a top 10 trend, but sat just off the podium. It appears that 2023 is the year the robots finally get their due.

Once considered a novelty, autonomous solutions, often simply referred to as drones and robotics, are getting their day. The megatrend is partly about automation of repetitive security tasks in lower-risk environments (think robots doing automated patrols in unstaffed facilities) and partly about highly responsive situational awareness (flying a drone to a remote or dangerous location for visual input back to the command post), but the real opportunity being seen for 2023 is connecting improved robotics with AI-embedded intelligence to finally put more "autonomous" in "autonomous devices," some of which required an operator to previously drive the robot. Notably the International Standards Organization narrowly defines robots to not include remote-controlled solutions such as remote-controlled drones and ground vehicles.

Today's autonomous devices, drones and robots are delivering multiple sensors and are able to interact with the built environment more than ever (robots that can navigate elevators, access readers and doors, and drones that can adapt to unfamiliar spaces where GPS is limited), and more and more major companies are investing in such solutions themselves or hedging their bets by funding start-ups and incubator projects in this area.

NEARLY 3.5 MILLION ROBOTS AND RISING

Over half a million industrial robots were installed in 2021 according to the International Federation of Robotics (IFR), and that doesn't even include robots for security applications, which are outside of the scope of the IFR's annual World Robotics research.

THE RACE TO INDOOR DRONES

One area where autonomous device technologies are showing great promise is with small, indoor drones. In November 2022, the U.S. Department of Homeland Security Science & Technology Directorate joined with Israel's Public Security Ministry to fund the work of two companies—one U.S. and one Israeli—to work together to develop an AI-powered indoor drone that could be used for emergency response situations such as fires, active shooter situations, earthquakes and other situations. Major U.S. security provider ADT demonstrated its indoor mini-drone at a recent tradeshow, and even in September 2021, Amazon made waves when it debuted its Ring Always Home Cam, a residential-quality mini-drone, which in late 2022 is still in invitation-only selling mode. Of course, such devices are already in use for inspecting confined spaces during non-emergency events, but strong advances in indoor location technology, photogrammetry and LiDAR, along with materials and designs that make the drones more collision tolerant, will propel this indoor mini-drone market opportunity.

THE SWARM IS COMING

Still largely in the world of military R&D, but in development from major firms like Lockheed Martin and others, are the AI-driven smarts that would deliver "swarms" of drones/unmanned aircraft systems (UAS). Alessandro Gagaridis of the US-based intelligence and security company Counterterrorism Group describes the technology in a June 2022 article for the Geopolitical Monitor:

"Drones operating in a swarm are all interlinked and in constant communication with each other. There is no clear threshold on the quantity of drones that must be connected to create a swarm, with figures ranging from a few hundreds to billions, also depending on their type and size. What is important is that they share information from their sensors and take AI-driven collective decisions toward the achievement of a single goal. This datalink and the AI software are therefore essential in creating the "hive mind" that defines a swarm and allows it to effectively function; and each single drone forming a swarm is just a small component playing a specific role in a greater system which self-coordinates the actions of its elements in a dynamic manner. Certain drones would use their sensors to locate and track targets, sharing the information with the rest of the swarm; others would perform jamming and electronic warfare tasks; another category would engage hostile forces, etc. The swarm as a whole would react dynamically to changes in the battlespace by performing complex non-linear and counter-intuitive maneuvers."

Fortunately notes, Gagaridis, "At present swarming remains largely theoretical and is still under development."

IMPACT TO THE PRACTITIONER/CSO

Input gained from top CSOs puts autonomous device impact in two camps. One is security operational value. The other camp is the risk impact of autonomous devices.

On the value side of the equation, some top corporate security teams report they are doing pilot projects of autonomous devices for security applications, but many more have noted that their general business operations teams are further ahead in adoption of autonomous devices, such as terrestrial robot usage to automate and monitor warehouse operations or using drones for remote visual inspection of hard-to-reach environments and infrastructure such as pipelines. Most note that they see the future value to security but are unable to justify the expense of early-stage products as of yet. Nonetheless, they do generally describe they see it not as an "if," but as a "when."

Regarding risk impact: Many top CSOs referenced risk from autonomous devices, particularly drone-based threats, and expressed frustration on the limited ability to deploy counter-drone measures (some sites/facilities do have such governmental authorization). They report constant concerns with operator-driven drones and are extremely wary of more autonomous solutions that will fly a pre-programmed path, and further afield, are considering the impact of swarm technology (see section below) that could overwhelm even the best procedures for defending against drone intrusions.

BY THE NUMBERS

855,000

Approximate number of registered drones in the U.S. as of March 2022

Source: FAA

This number is widely considered by drone industry media to be underreported by the FAA, and over 321,000 of those registrations were commercial in nature.

MEGATREND 10

PROLIFERATION OF SENSORS

MEGATREND MOVEMENT

The proliferation of sensors trend was first voiced by SIA Security Megatrends Advisor Tara Dunning of Wesco and was warmly received by the SIA members who responded to the 2023 Security Megatrends survey, earning it a spot on the list.

"With the proliferation of IoT, the need for a greater diversity of sensors has exploded across all industries." So wrote Robbie Paul, director, IoT business development at electrical component distributor Digi-Key Electronics, for EP&T magazine in 2020. Today, accelerometers can detect vibrations that might indicate dangerous conditions. Easily deployed sensors can deliver temperature status that can be used to make buildings more efficient or indicate safety issues.

This megatrend speaks to rapid "sensorization" of the built environment to support smart building/smart city projects. It's seen not just in the rapid expansion in the number of camera sensors but in the growth of sensors like LiDAR, radar, air quality and chemical detectors, moisture sensors, energy sensors, temperature sensors, audio sensors, people counting sensors, motion detectors and even accelerometers that can detect vibrations, explosions and earthquakes.

One way this proliferation has been impacting security is that, as customers have demanded more sensor inputs, security device makers have creatively found ways to turn common sensor inputs like cameras and microphones into smart sensors. Emerging examples are AI-powered video systems that can recognize spills and flooding, or audio sensors that can not only record, but can automatically detect aggressive voices, gunshots and other such abnormal audio signals.

IMPACT TO THE PRACTITIONER/CSO

Just what a practitioner needs, more data points to have to analyze. But the reality is that leading practitioners have always been data hungry—if they can put meaning to that data. The trend has always been lurking in the industry, as seen in the steady growth of deployed cameras (an estimated 84.5 million cameras are in active use in the U.S. according to research from October 2022 produced by Omdia exclusively for SIA), and more intrusion and access data inputs. Today, practitioners are opening their eyes to emerging sensor solutions at their disposal (vape detection, harmful gas detection, etc.) and many firms are starting to view all the sensor data as inputs for managing the status of their business and facilities, not just for security.

Additional Member Resources

SIA Guide to School Security Funding

U.S. Physical Security Market Assessment

Changing the Channel: Drones and Robotics

Proptech Report: Commercial Real Estate

SICC SECURITY INDUSTRY CYBERSECURITY CERTIFICATION

Security Industry Cybersecurity Certification

CSPM CERTIFIED SECURITY PROJECT MANAGER

Certified Security Project Manager

Data Privacy Code of Practice: Video Surveillance

Reducing Risk, Seizing Opportunity: A Guide to Privacy

Safe and Sound: Audio and Intelligent Communications

Find these resources at:
securityindustry.org

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