2022 SECURITY MEGATRENDS™

THE ANNUAL VISION FOR THE SECURITY INDUSTRY

SIA
SECURITY INDUSTRY ASSOCIATION

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
Author, 2022 Security Megatrends Report
gkohl@securityindustry.org

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

MARC BENSON
Associate Director of Membership
mbenson@securityindustry.org

JOHN COLEMAN
Manager, Member Services
jcoleman@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

2022 SECURITY
MEGATRENDS™

THE PROMISING FUTURE

SIA's annual Security Megatrends report is a story of how our industry will be changed, but it's more a vision of how our industry will drive change. Based on industry surveys and focus groups, plus drawn from insights that speakers shared during our annual Securing New Ground (SNG) conference, this is our best forecast for what opportunities lie ahead.

Now in its sixth year serving as the industry's defining list of trends, Security Megatrends is a consistent, measured report, and if you compare this year's list to our 2021 report, you won't see a full sweep of the trends. The megatrends aren't a rally cry for the latest buzzwords; rather, these are the long-term trends that change the underlying archetypes.

Artificial Intelligence (AI) continues to reign as the #1 megatrend, and each year, this trend moves further along its developmental journey. While AI may have once been simple marketing hype from companies seeking promotional value, today the application of AI (mostly in the form of machine learning) is a real part of most company's next generation solutions, correlating data that had been heretofore uncorrelated and automating one or two more processes or steps to make a business owner or a security officer's job that much easier.

Cybersecurity likewise stayed consistent, still ranked #2 for the 2022 report, propelled perhaps by the constant fear of a security solution held hostage by ransomware or of a nation state hacking a vital government or critical infrastructure security system. Today, cybersecurity is a market differentiator, and entire segments – notably in the field of video surveillance – have been transformed by attention to cybersecurity. Before you turn the page and we reveal the full list of 2022 Security Megatrends, I do want to recognize three trends that represent a mindset shift within the industry. One is Increased Interoperability (ranked #6), one is Data Privacy (ranked #7) and the other is Health & Sustainability (ranked #10).

In recent years, the industry has been more cognizant of how security solutions shape the world, and we believe this will only increase in the future. Today we ask, are we making the world more closed, or are we helping to open the world? Asked in another way: Are we just restricting (keeping bad people out) or are we enabling (ensuring the right people can get in)? Simultaneously, the industry has made commitments to ethics, not just in how security solutions are used but in how individuals' privacy is protected in these systems.

Today, the fact that three of the top 10 trends are centered around openness, respect of individuals and how we make the world both healthier and more sustainable speaks to the level of change that has occurred in our industry. And that kind of change can only lead to an ever-brighter future!

Sincerely,
Pierre Trapanese
Chair, SIA Board of Directors

THANK YOU

SIA THANKS ITS 2021 SNG SPONSORS

ALLEGION

AMAG TECHNOLOGY

ASSA ABLOY
The global leader in door opening solutions

AXIS COMMUNICATIONS

BOSCH

brivo
simply better security

convergint

DELL Technologies

dormakaba

Genetec

Imperial Capital

intel

LENEL·S2

milestone

PROSEGUR

RAYMOND JAMES®

SALIENT

INDUSTRY PARTNER

ISC

MEDIA PARTNERS

Campus Safety

SDM

SIW SECURITY INFOWATCH.COM

SECURITY SYSTEMS NEWS

SECURITY SALES & INTEGRATION

SECURITY

EXECUTIVE TAKEAWAYS

"Technology is moving at an incredible pace, and so have our customers' needs. Our customers have now really focused on innovation. We're seeing companies wanting to move to cloud-based solutions. They want to modernize their network, security infrastructure, remote capabilities. We're seeing an increase in disruptive technologies like AI and computer vision. Businesses are continuing to prioritize digital transformation initiatives and get real-time data to make better decisions."

– Bhuvana Badrinathan, CIO, Convergint

"Cybersecurity and IT generally are integral to smart buildings. These are part and parcel of the whole thing. If you want to call it a smart building, then it has to be a smart and secure building."

– Adam Chapman, Cybersecurity Manager and Product & Solution Security Officer, Siemens

"It [AI] is the natural evolution of our industry. In the end, it's about how we can drive operational efficiencies."

– Luis Orbegoso, President, Americas, Allegion

"B2B industries are way behind all the consumer product companies, so we're basically fighting for the scraps [in the supply chain]. I'd love to tell everyone that 2022 is going to be great, but I think you're going to see some struggles throughout the year, and there might be some light at the end of the tunnel, but I don't think so for another 12 months unfortunately."

– Thomas Cook, Executive Vice President of Sales & Operations, Hanwha Techwin America

"80% of the spending in the security industry today is manual labor. That means guards, monitoring or even installation services. That will change."

– Fredrik Nilsson, Vice President, Americas, Axis Communications

"People don't mind change. They mind being changed. And when there's a pandemic or there's a disaster, there's going to be a lot of change."

– Bonnie Michelman Executive Director of Police, Security and Outside Services, Massachusetts General Hospital and Mass General Brigham Corporation

"I call it the 'OK, now what?' type of data, where it's the aggregation of data that triggers an action."

– Lee Odess, General Manager of New Market Development, Latch

"It's kind of the elephant in the room that when you build products, it's not entirely built by the company that you bought it from. There are a lot of third-party components, sometime open-source components. They can come from many places, so you need to track this somehow as a supplier, but also as a customer."

– Mathieu Chevalier, Principal Security Architect, Genetec

"When you think about all that's going on across some of the major sectors of the market, access control, video, even guarding, we are seeing tremendous amounts of change – business model transformations, the infusion of technology at levels that this industry has never seen before, the development of businesses like some of the SPAC companies, or the companies that have gone public through SPACS, that are very nascent in what they're doing, but they're trying to transform entire industries. So the excitement level in this space from the investment community is extremely high. It's the highest I've seen it in quite some time. For companies in the space, I think you're in a good spot. There's plenty of capital out there, so continue to go do what you're doing because you've built up the business and the industry in a very good way. There's more forward momentum and progress in our space than ever before."

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

HOW WE DEFINED AND RESEARCHED THE 2022 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 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 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 2021 SNG conference 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 2022 SIA Security Megatrends report, but also provided you insights and action items to facilitate a successful future in the security industry.

2022 SECURITY MEGATRENDS

MEGATREND 1

ARTIFICIAL INTELLIGENCE

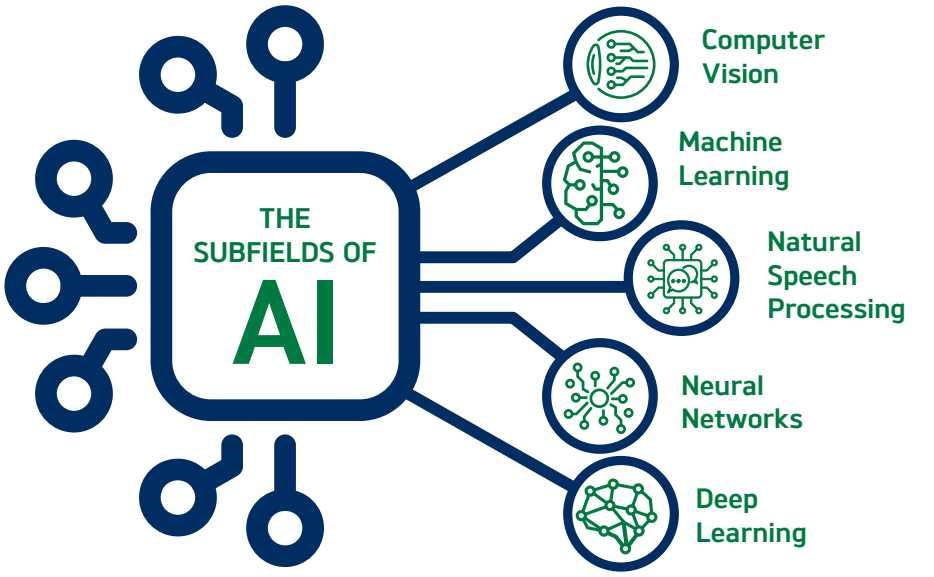
THE KING CONTINUES TO REIGN. In the 2021 Security Megatrends report, artificial intelligence (AI) rose to the position of the top-ranked megatrend, and despite coups attempted by would-be successors of cybersecurity, supply chain, RMR models and even long-term workforce development challenges, all attempts to dethrone king AI ultimately failed and AI remains atop our 2022 list. Long live the king, you might say, as industry firms have embraced the promise of AI, whether that be through advance audio analytics, complex facial recognition and cutting-edge video surveillance scene processing that can recognize human behaviors – and, of course, the world of robotics and drones.

The cynics may say it is as much a marketing trend as it a technology trend, but AI is indeed a real industry shaping (and shaking) trend today, even though the more measured and less-boosterish technologists in this space will admit that a lot of what purports to be AI today wouldn't quite meet the threshold of true "intelligence" and is fundamentally just preprogrammed algorithms doing computer vision-based object detection (e.g., vehicle in scene, license plate recognition, face mask detection). Real AI, they might say, is when a machine can far exceed the capabilities of human intelligence or can even apply the lesson learned in one situation to another, entirely different situation. Without a doubt, there are solutions today that exceed those human capabilities, like the facial recognition systems that return a high probability match from a large database nearly instantly.

AI in this industry has always existed on a spectrum, from basic smarts that can occur in a compact security camera's on-board chip to the level of intelligence that requires extensive server arrays and which can process truly massive amounts of unstructured data. Today, much of what is occurring in the industry is in the realms of computer vision, machine learning and even some natural language processing, but the

prospect of neural network-powered machine learning and deep learning means even deeper insights from more complex and less structured data.

And as we concluded last year, "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."



Source: SAS Institute

PERSPECTIVES

"Artificial intelligence would be the ultimate version of Google. The ultimate search engine that would understand everything on the web. It would understand exactly what you wanted, and it would give you the right thing. We're nowhere near doing that now. However, we can get incrementally closer to that, and that is basically what we work on."

–Larry Page, Co-Founder of Google

"The way researchers break platforms is they do things that they already know are not supposed to happen. And they wait to see what happens with the device. So how do you validate that? How do you test for all those completely oddball things? That's where AI can really help with some of the validation and be able to do these nonsensical tests on the device and help us in ways that maybe humans wouldn't have even thought of, or if we had, it would have taken a long time, and we can speed up that validation process."

– Tom Garrison, VP & GM, Client Security Strategy and Initiatives, Intel Corporation

IT'S ARTIFICIAL, NOT AUTOMATIC

The machine may be learning, but who is doing the teaching? AI researchers and technology developers will tell you that the amount of work that goes into training an algorithm is often a staggering effort of not only generating a massive set or organized data for the algorithm to process, but also requires a massive human effort of providing nuanced feedback to the algorithm so that the algorithm can improve its accuracy.

As Saif Khan and Alexander Mann wrote in their 2020 paper for the Center for Security and Emerging Technology titled "AI Chips: What They Are and Why They Matter," "the success of modern AI techniques relies on computation on a scale unimaginable even a few years ago. Training a leading AI algorithm can require a month of computing time and cost $100 million."

ARTIFICIAL INTELLIGENCE *(continued)*

AI SHAPING HUMAN GUARDING

Allied Universal CEO Steve Jones tells the story of how AI is making security officers even more efficient:

"We have built out a handheld technology that our officers use every day to track their performance and what they do and be kind of the checklist of things that they need to do. The AI takes all the data that we're collecting and goes through and makes recommendations on where our officers should go. In the old days we would put together all these reports manually in writing by pen and paper, and then we would consolidate these things and we'd try to present to corporate security directors and try to figure out what we need to do for our enterprise to better secure it, keep our people safe and protect and minimize risk. Now suddenly, the AI is doing that. As we are entering data on the handheld device, the AI is giving us real-time information.

"We're using it internally to operate our business, helping us drive metrics in our business and taking on menial tasks that we used to do all the time. The artificial intelligence engine is learning how we do those things day in and day out with thousands and thousands of employees. And now it's able to do it."

$15.6T
Potential contribution to the global economy by 2030 from AI

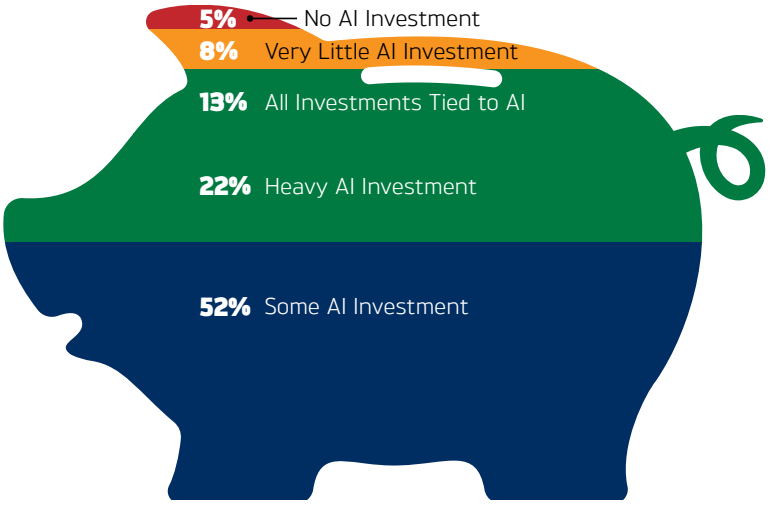
14.5%
Percentage of North America's GDP that AI could influence by 2030

Source: PwC Global Artificial Intelligence Study

SNG POLL

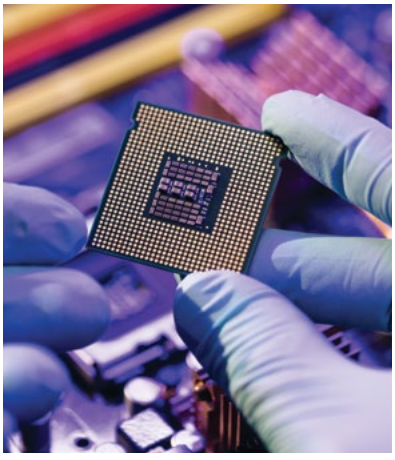
HOW WOULD YOU CHARACTERIZE YOUR FIRM'S R&D INVESTMENTS RELATED TO APPLYING AI TO YOUR PRODUCTS AND SOLUTIONS?

AI investment from security industry companies is exploding. When we first surveyed SIA member companies in 2019 about their R&D investments into AI, less than 2% said that all R&D investments were tied to AI. In 2020, that percentage crept up to 3%. But sometime in the last year, what started as an ember is now a raging fire of investment into AI, with 13% of companies saying that all their R&D investments are tied into AI opportunities.



CHALLENGE

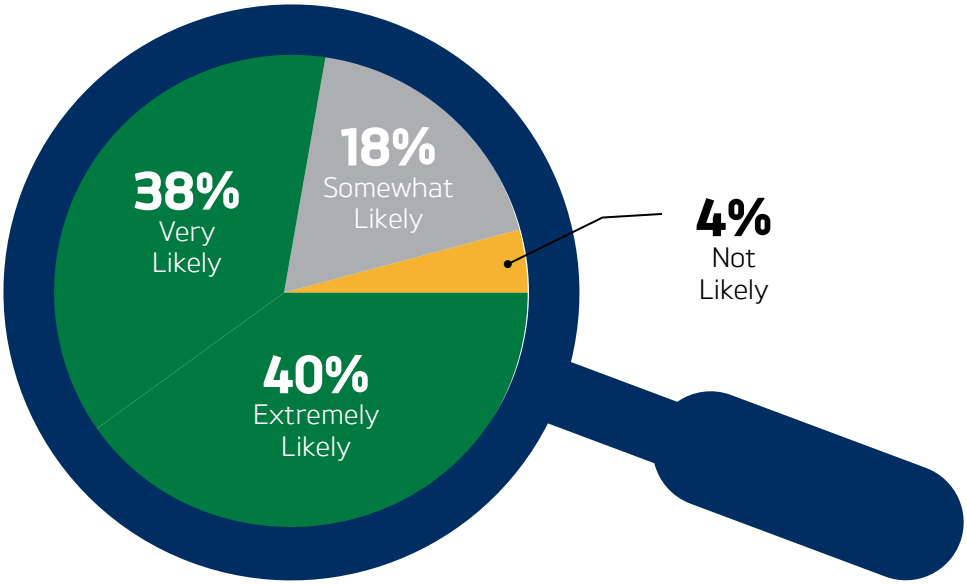
It's often claimed that Moore's Law is coming to an end, referencing the famed prediction in 1965 by Gordon Moore that the number of transistors on a chip would double every two years, effectively doubling computing power. As David Rotman noted in the February 2020 for the MIT Technology Review, the rate of development is slowing, even as our demands for computing power grow. How do we reconcile those two seemingly incongruous destinations? Experts say there are two paths. The first is to simply buy more on-demand processing, such as through cloud services. The second option is to make the algorithm or software performing the AI more efficient. Still others, particularly those in the world of chip manufacturing, will says that a slowing rate of processing power from exponential growth to sub-exponential just means computing power growth is slowing, but that the growth is far from over, and that specialized AI chipsets doing parallel, simultaneous processing (versus sequential processing) will pick up the slack that previously required the ability to shrink transistor sizes to fit more processing on a chip.



SNG POLL

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

Recognized as its own Security Megatrend in the 2021 report, for the 2022 report, predictive data analytics is included within the broader trend of AI. Predictive data analysis aligns well with the AI fields of deep learning, which promises to be able to autonomously identify patterns out of large data sets, and neural network computing which can identify patterns from undefined data. Even the simplest predictive applications can be business altering, such as recognizing when hardware needs service or will require replacement.



MEGATREND MOVEMENT

Ranked second in 2020 and fifth in 2019, artificial intelligence jumped to the No. 1 spot in 2021 as this trend was perceived as the trend that would ultimately drive most technology advances in coming years. It remains there for the 2022 report.

TAKEAWAYS

AI is not universally defined, and AI is best viewed as specific subfields of development, ranging from computer vision to deep learning.

Development of AI-specific chips is propelling new advancements.

This Megatrend promises to influence every sector of security, from guards to drones to identifying solutions through big data processing – even validating device cybersecurity by providing comprehensive scenario testing.

MEGATREND 2

CYBERSECURITY

IN LAST YEAR'S REPORT AND IN YEARS PRIOR, we named this Megatrend the "Cybersecurity of Physical Security," but we're expanding the perspective further. Maybe it was the Colonial Pipeline attack that led millions of Americans to experience fuel shortages – or other prominent ransomware attacks on companies like Acer, Brenntag, JBS Foods and even Kaseya. But our industry's concern isn't just with the cybersecurity of physical security; it's at least with cybersecurity of operational technology (OT), but truthfully, it's a concern with cybersecurity in general, because the attack vector may not always be an access control server or a security camera; it could be your own corporate servers or a piece of network infrastructure you added to build a client's security network. And what's more, while the AI megatrend may be the shiny new object that holds future promise, the cybersecurity megatrend is that nagging worry that no matter how good you are, if you make just one mistake, everything you built could be exploited for ill.

But cheer up, because awareness of cybersecurity has changed dramatically within the industry, and there are indications that many buyers – at least those with strong IT and cybersecurity focuses themselves – are asking the right questions to validate a company's cybersecurity approaches and are simultaneously willing to pay a premium for products that offer better protection.

PERSPECTIVES

"The threat landscape is evolving at an equal, if not faster pace than technology. And it's essential that companies implement best practices with respect to cybersecurity solutions in their ecosystems."

– Bhuvana Badrinathan, CIO, Convergint

"We make locks, and our expertise is with that mechanical lock and making sure that people don't get in. Now that lock is connected, our expertise has to be with cyber as well and the firmware that goes in there. I think it [cybersecurity] is going to be the ticket to play going forward. If you want to be connected, you're going to have to have a secure infrastructure or else people won't trust you."

– Luis Orbegoso, SVP & President, Americas, Allegion

"We have hundreds of some of the leading security researchers in the world, working on our platforms. We challenge them to try to break our own platform. We try to find security vulnerabilities that no one else in the world has found. And by doing that research first, when we find them, we fix those issues whether they're on our future products or even on our existing products that are out in customers' hands. We invest significantly to stay ahead of the people that are trying to do harm to the platforms. But we not only do that, we then need to work with our partners and the ecosystem to validate the fixes, to make sure that they work as they're supposed to work, and that they don't cause other damage."

– Tom Garrison, VP & GM, Client Security Strategy and Initiatives, Intel Corporation

"I call it social accountability. Even if you don't have a CISO, I think it trickles down to all the employees in your enterprise. You have to start training everyone to realize that they're not only affecting themselves, but they are affecting the entire enterprise. It trickles down to the rest of the employees to empower them to say, 'Hey, look, you are ultimately responsible for any theft or any compromises or any problem that is coming from whatever you're doing.'"

– Min Kyriannis, CEO, Amyna Systems

ATTACKS TARGETING OT

Many cybersecurity analysts say that the new field of attack is OT, and attackers often pursue a strategy of ransomware on these critical systems, as the Colonial Pipeline incident of 2021 evidenced.

Why? As Genetec's principal security architect, Mathieu Chevalier, explained during SNG 2021, "OT is generally less mature from a cybersecurity perspective compared to other IT systems that we're using… Maybe you have legacy systems. Maybe they are hard to patch. Maybe the availability is super important, so you don't want them to go down, and you might not have a failover strategy."

> **"One way to defend legacy systems** is a defense-in-depth strategy that layers multiple protections to mitigate exposure."
>
> *– Wayne Dorris, Cybersecurity Business Development Manager, Axis Communications*

Wayne Dorris, cybersecurity business development manager for Axis Communications, says the problem is especially relevant in the world of interconnected building systems, where products may be installed for "7, 10, 20, even 30 years." These legacy OT systems often don't match up with typical IT considerations, and it makes it even more challenging for the responsible team – the customer, integrator and manufacturer/solution provider – to ensure that these solutions are continually sustained from a cybersecurity standpoint.

Chevalier says short of replacing old systems, one way to defend legacy systems that can't be brought up to today's cybersecurity protections is a defense-in-depth strategy that layers multiple protections to mitigate exposure of these older platforms.

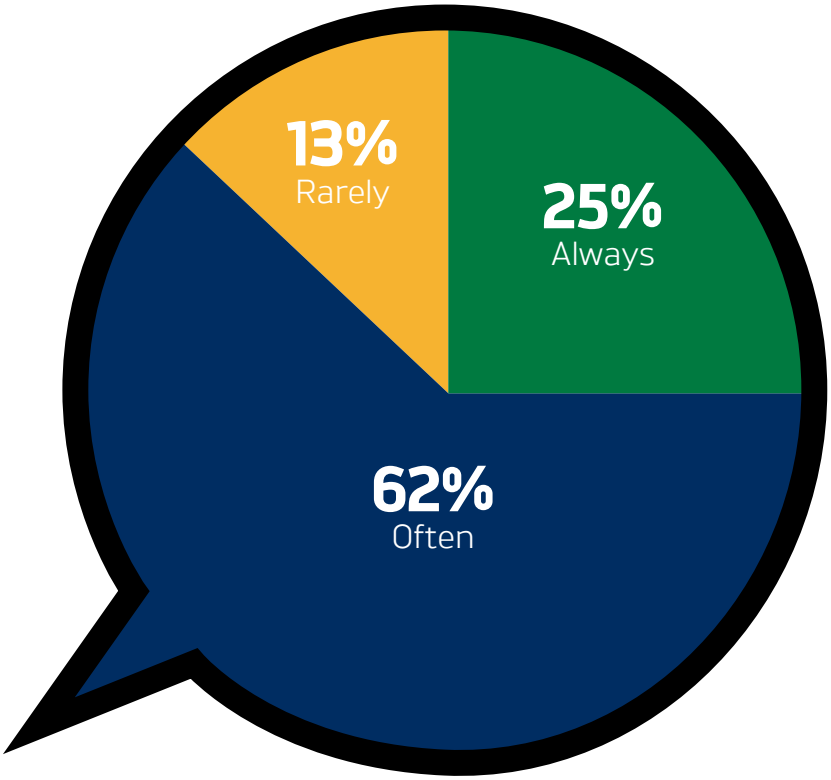
INTEROPERABLE RISK

With increased interoperability (Megatrend #6 for 2022) comes an expanded attack surface. As companies use APIs to bring in additional data sources or integrate with other platforms and software, the challenge of vetting those services intensifies, and solution and integration providers will need to disclose those API-integrated services or date sources, or at least advise their customers of those connections.

SICC™ SECURITY INDUSTRY CYBERSECURITY CERTIFICATION

MORE TRAINING, LESS RISK

While many industry leaders note that the industry is still in dire need of cybersecurity training, particularly for field installers and technicians, there are indications that security technology companies are strongly investing in cybersecurity training for employees. Simultaneously, certifications like the Security Industry Cybersecurity Certification (SICC) developed by SIA with support from PSA Security Network and Security Specifiers are gaining a foothold in the industry, along with more broad-spectrum cybersecurity certifications from organizations like (ISC)².



SNG POLL

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

Cybersecurity conversations are shifting, explains Mike Dunn, chief technology officer (CTO) of Prosegur USA. He notes that as ransomware and other cyberattacks on operational technology and IoT device systems have made more news, companies like his are no longer always having to bring up the cybersecurity topic or educate and remind customers of the need for a defense strategy for their physical security systems and other operational technologies. The conversation flipped, he said. "It shifted during the pandemic at some point with them saying, 'Please, what can you give us? What do you have for services? How can you help us and protect us?'"

The chart above reflects that shift. In our previous year of tracking this benchmark question, SIA found that 2% of respondents said cybersecurity was never a discussion point; today, zero respondents indicate that cybersecurity is ever not discussed during customer calls. While a year ago, cybersecurity discussions were "often" part of the conversation 52% of the time, today that frequency has increased to 62% of the time.

AI'S PROMISE FOR CYBERSECURITY VALIDATION

While AI-enabled systems, with their extensive access to data and high value for an organization, are a rich target for cyberattacks, AI itself also has the promise of being useful for cybersecurity validation.

"Security is not about testing whether a product works the way it's supposed to work," explained Intel's Garrison. "The way researchers break platforms is they do things that they already know are not supposed to happen. And they wait to see what happens with the device. Does it fail in a certain way that maybe unlocks something that wasn't supposed to be unlocked?"

Unlike traditional cybersecurity testing, which relies upon human creativity and effort to test the cybersecurity of a device, Garrison said AI can help with validation by rapidly performing nonsensical tests that humans would not have thought of or would not have had time to test.

83%

Percentage of organizations which suffered an operational technology (OT) cybersecurity breach in the 36 months prior to November 2021

73%

Percentage of CIOs and CISOs who are "highly confident" they will not suffer an OT breach in the next 12 months

Source: Skybox Security research

MEGATREND MOVEMENT

Cybersecurity was ranked No. 1 in 2020, then slipped to No. 2 for 2021 as AI claimed the top slot. For 2022, it holds steady, indicative that cybersecurity is not something that you can ever forget about.

TAKEAWAYS

Attacks targeting operational technology (OT) are increasing.

OT systems are ripe for attack both for their business impact and because such systems are less likely to be updated, patched and refreshed at the rate of typical IT platforms.

Industry needs to retain its commitment to cybersecurity training for field workers.

MEGATREND 3

SUPPLY CHAIN ASSURANCE

THERE ARE TWO TYPES OF SUPPLY CHAIN CONCERNS shaping the industry's future.

The first is a logistics challenge – the ability to obtain source components, raw materials and even finished products. The disruption lies in many places. Temporary shutdowns for some manufacturing operations led to cascading shortages when the economy rebounded faster than anyone could predict. Complicating the situation are labor shortages that affect the entire supply, from manufacturing through shipping and distribution, to even the labor necessary to install products if you can get them.

And there's no indication that all these problems will just unravel as quickly as they formed. Inside the industry, executives are cautious to hope for any complete resolution to the logistics delays before the end of 2022, and supply chain strategists outside the industry, like Manish Sharma, group chief executive of operations services at the consulting firm Accenture, have said "Our findings indicate the disruption could be for up to three years" (New York Times, Nov. 29, 2021).

The second supply chain concern, some say, may be even more important, and it's closely related to our #2 Megatrend of cybersecurity. The concern is the ability to put full trust in the source code, firmware, system-on-chip and other hackable elements that exist with any product or solution. As addressed in the 2021 Securing New Ground keynote by Intel's Tom Garrison, the challenge today is to build transparency and traceability of the code and subcomponents of any solution, so that the end customer can trust that the installed device, software or solution is precisely what they expected.

Thus the 2022 SIA Security Megatrend of "supply chain assurance" is a blended trend that mixes logistics with cybersecurity, and the industry is paying more attention to this trend than ever before, as indicated by its first time being ranked among the industry's megatrends.

PERSPECTIVES

"The more control you have over your own supply chain, the better."

– Scott Paul, President, Alliance for American Manufacturing

"B2B industries are way behind all the consumer product companies, so we're basically fighting for the scraps [in the supply chain]. It's a struggle. I'd love to tell everyone that 2022 is going to be great, but I think you're going to see some struggles throughout the year, and there might be some light at the end of the tunnel, but I don't think so for another 12 months, unfortunately."

– Tom Cook, Executive Vice President of Sales & Operations, Hanwha Techwin America

"Supply chain is the next frontier from a security standpoint."

– Tom Garrison, VP & GM, Client Security Strategy and Initiatives, Intel Corporation

DIGITAL DNA

In his keynote at Securing New Ground, Intel's Tom Garrison shared the firm's vision for the "Digital DNA" of a device.

"What we mean, quite simply, is you should understand everything about the device. If you think about something like human DNA, today we can track people's relatives and ancestors back hundreds and in some cases thousands of years. So, why can't we apply the same sort of thinking about our technology devices and be able to track back and trace back the components of the devices? And are these devices in a trusted state or not?"

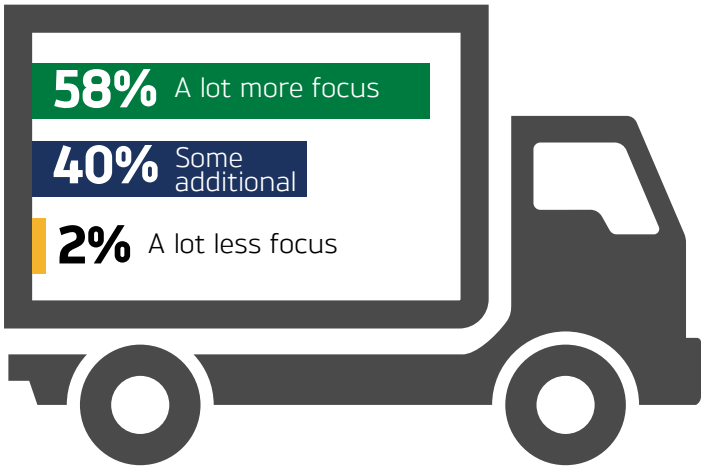
For Intel, that information will be stored on the device and protected with a cryptographic key that is individual to each device.

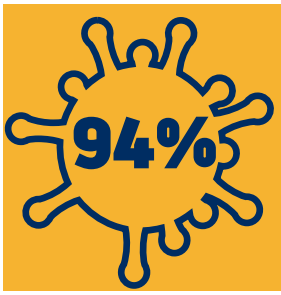
"We're capturing all the specific components that were built for that specific device," explained Garrison. "We're signing it with that specific endorsement key, which is unique for that platform. And by signing that information, then we can store that information in the cloud. As the device now moves its way through the transportation chain, ultimately to your site or to the end customer site, then the device can now be pulled or tested to say has anything changed in that device from when it was built? Because we can test there, locally. We compare it to the results we had when we first built it, and we say, has anything changed? If it has, we alert the user or IT and they can make a decision how to proceed or not."

SNG POLL

ARE YOU PLACING MORE FOCUS ON YOUR SUPPLY CHAIN TODAY VERSUS 2 YEARS AGO (PRE-PANDEMIC)?

Call it the "chart of no surprise," but 98% of companies in the industry have invested more time and focus on their supply chain than they did pre-pandemic, with more than half saying they're giving their supply chain "a lot more focus." In surveys of the SIA membership conducted in October and November 2021, supply chain was among the top concerns of executive respondents.





Fortune 1000 companies seeing supply chain disruptions from COVID-19

Source: Accenture

58%

SNG attendees who said that supply chain delays is the factor most likely to negatively impact their business this year

Source: SIA, SNG 2021 research

MEGATREND MOVEMENT

A new megatrend for 2022, the supply chain has been a consistent immediate concern for SIA members in recent surveys and conversations. And while the microchips will someday be back in stock, the real lesson here is that your supply chain can never be taken for granted.

TAKEAWAYS

Supply chain delays are expected to continue throughout 2022.

Supply chain assurance has a direct relationship to cybersecurity in terms of the trust of subcomponents and code provided by outside parties.

The challenge for supply chain is to provide transparency and traceability.

Even companies that don't sell hardware, such as VMS providers, are facing challenges because the installation and integration of their software requires servers, cameras and other hardware as part of the systems.

MEGATREND 4

SERVICE MODELS AND THE CLOUD

THE "MOVE TO SERVICE MODELS" and "cloud computing" have long been included in SIA's annual Security Megatrends report as separate trends, but for 2022, based on input from survey data and commentary during Securing New Ground, we're officially connecting these two megatrends.

"The move to service models has been kind of concomitant with the move to the cloud," explains Steve Van Till, Brivo's president, "but really it [service models] is a business concept as opposed to a technical concept [cloud computing]." The fortunes of these two trends have often been tied together, and one way many firms have been able to move to as-a-service/recurring revenue models has been by delivering solutions in the cloud.

Today, this is a trend that nearly all companies in the industry are exploring, and it's becoming uncommon to see a startup company launch without a subscription delivery model and some element of the cloud, whether it's a solution delivered entirely via the cloud or whether the system uses the cloud for some processing or storage.

PERSPECTIVES

"I basically say, 'Listen, you're talking about owning and renting. You have a car; you either own the car or you lease the car.' So that's the only thing we're changing on you is that you're now leasing a product that's at your site, whether it's an NVR, DVR or a camera in our video world. And you're going to pay for that on a monthly basis or a yearly basis, instead of buying it one time, so it's OPEX versus CAPEX. And again, do I want to lease the car or do I want to own a car and deal with the maintenance? And that's typically what an IT guy understands. It's the security people that grew up in the industry [before service models]; they're the ones that are confused about [this change to a service/leasing model]."

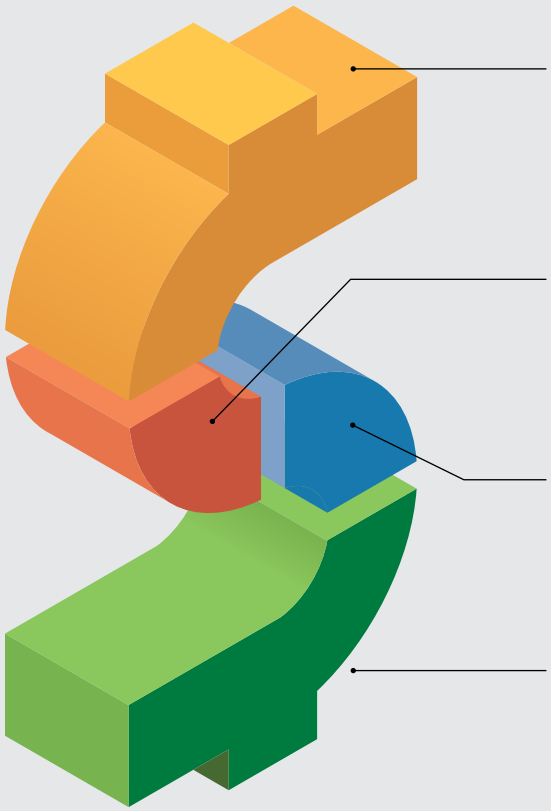
– Tom Cook, Executive Vice President of Sales & Operations, Hanwha Techwin America

"There are clearly much higher valuations for companies with recurring revenue models. Witness that security integrators with mostly one-time install revenue will trade for 0.5 - 1.5x revenue while recurring-revenue-focused alarm companies will trade for 3 - 5x annual recurring revenue or ARR. And then in the high technology SaaS businesses which are heavily recurring revenue focused, you can see revenue multiples of over 10x."

– John Mack III, EVP, Imperial Capital

SERVICE MODELS AND COMPANY VALUATIONS

Imperial Capital's John Mack III says the key variables for recurring revenue businesses to trade at higher multiples include the following attributes:



1. **Reasonable investment level to create new customers.**
   "In the alarm industry this is called 'creation cost.' In the SaaS world, this is measured with a metric known as LTV/CAC, long-term value creation/customer acquisition cost."
2. **Good gross margins for the recurring services.**
   "Typically, at least 60% but more like 70%+ and for the high technology SaaS businesses, in many cases 80%+."
3. **Low attrition (10% or less) or high retention (90% or better).**
   "In many cases, with new services sold to existing customers there is net growth in recurring revenue or net retention over 100%."
4. **High growth rates.**
   "Rates of at least 10%+ in recurring revenue per year and for the high valuations growth, rates in the 25%+ range or much higher."

MEGATREND 4 SERVICE MODELS *(continued)*

AS-A-SERVICE MODELS, NOT JUST SERVICE AGREEMENTS

Service models do not equal service agreements stresses PSA Security Network CEO Matt Barnette. Typically service agreements were a small addition on top of a one-time project-based fee. And while service agreements are a step in the right direction for integration companies looking to transition to a recurring revenue model, the real change comes when the former project-based fee is transformed into a recurring charge.

BETTER FOR BUSINESS

At SNG, Luis Orbegoso (who today leads Allegion in the Americas) tells the story of when he worked at ADT and the company made the switch to the cloud for delivering video solutions: "We actually stopped selling DVRs for the most part; [we] put all the video in the cloud. [It] drove a huge amount of retention. It was a better business model. It was easier to sell because it was less of a capital expenditure."

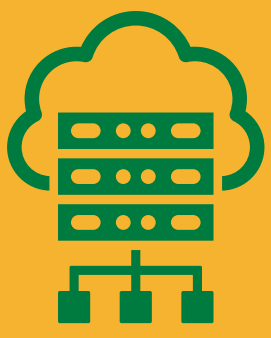
UPTIME, EVEN DURING BAD TIMES

As the COVID-19 pandemic sent workers home, it sent company CTOs scrambling to ensure systems remained available, whether the worker was in a cubicle on office floor 7 or working from their dining room table or a corner of their bedroom. Cloud solutions naturally exploded in popularity.

GENERATIONAL CHANGE TO RMR

Chris Meiter, president of Salient Systems, tells the story of changing from perpetual licensing to a subscription model.

"We're seeing a major transition from what we classify as the perpetual licensing agreement, to a subscription-based model," said Meiter. "The customer sees the value of the upgrades and things that come with that subscription model on an annual basis. But as we first rolled this out, we actually had some pushback by some of our integrators that were like, 'Hey, I've been selling perpetual, and we don't see the value in subscription-based.' It was literally this one company, a 50-year-old company, which had been selling perpetual licenses forever.And that was the first generation of the company speaking to us, but all of a sudden, the second generation says, 'Hey, wait. We want to build the value of this company. We want to have more equity value in this company. You can't do it just with a one-and-done sale. You need to do it with a recurring model.' And they ran that through their CFO and they could double- or triple-increase their company's value within two years by moving from perpetual licensing to subscription-based software. So, the message is getting out there and they're seeing the value."



50%
Percentage of corporate data now store in the cloud

Source: Statista

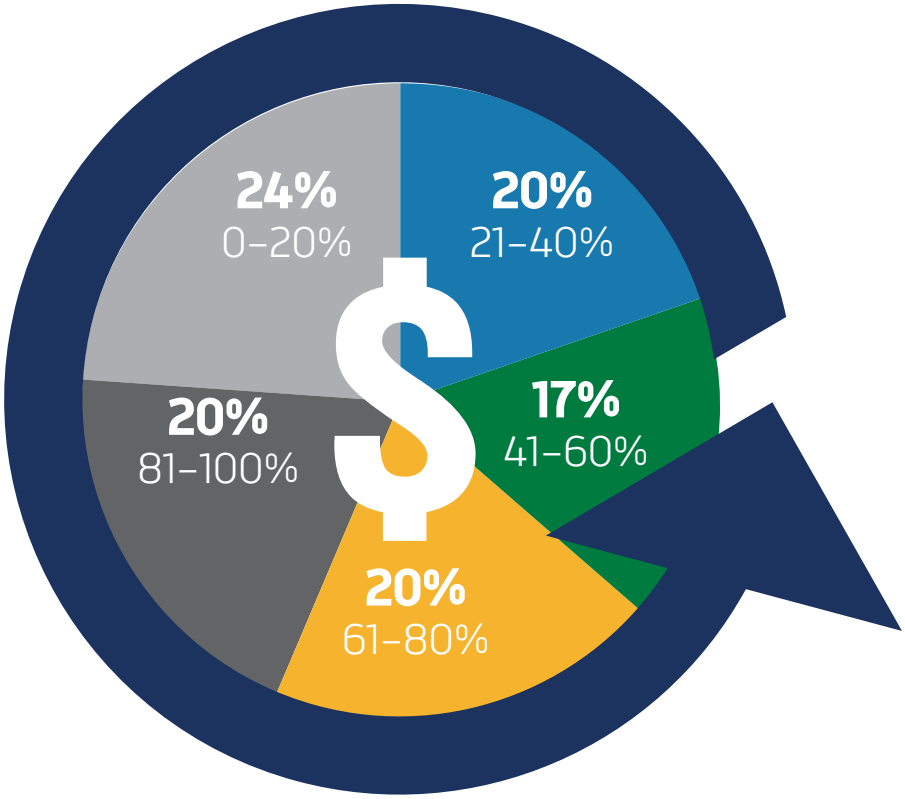
98%
Percentage of companies that had at least one cloud data breach in the past 18 months

Source: IDC

SNG POLL

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

Business models continue to shift. A year ago, over a third of respondents said that less than 20% of their firm's total revenues were attributed to recurring revenue. A year later, that number had decreased to less than a quarter of respondents, indicating that companies were steadily transforming their business revenue from one-off sales to recurring, as-a-service income streams.



MEGATREND MOVEMENT

A long popular Megatrend, the move to service models had ranked #5 in 2017 and 2018, falling to #7 in 2019, #9 in 2020 and #10 in the 2021 report. Meanwhile, cloud computing had seen its ranking steadily climb, but the jump into the #4 position for 2022 reflects both the effect of the pandemic and conjoining of what were previously two separate megatrends.

TAKEAWAYS

Investors, equity firms and even companies making acquisitions continue to deliver higher valuations to companies which are heavily invested in cloud services and recurring revenue.

Companies with software services or access to data services can make the cloud and recurring revenue business model transition easier than hardware-only type companies.

Security end users requests for anywhere, anytime access to security solutions will further advance cloud adoption.

Many formerly "on-prem" software-and-server based security solutions now are configured to run on common cloud infrastructure platforms from firms like Amazon Web Services, Google and Microsoft.

MEGATREND 5

WORKFORCE DEVELOPMENT

IN BOTH THE SURVEY RESEARCH done for this year's Security Megatrends report and in the fall 2021 SIA Membership Survey, it was clear that one of the biggest pain points to security industry leaders and companies of all type in the industry is the ability to find the talent they need. Members said it was a broad-spectrum problem, impacting manufacturing, software development and sometimes sales. But consistently, the biggest area of pain was from integrators who were challenged to find competent installers and technicians.

That inability for integrators to find the workforce they need has a snowball effect on the industry; it limits these companies' ability to install products and complete customer job requests, which in turn can affect the security of their clients' site, and it creates a bottleneck on potential sales for every company in the security technology business ecosystem, particularly the manufacturers, solutions developers and distributors which depend on sales and project completions by the integrator channel.

The industry is also plagued by the ongoing global shortage in cybersecurity workers, which puts the cyber protection of physical security solutions at risk, and many of SIA's members have voiced the challenge of hiring competent software and application developers, too. Unfortunately, the problem of not enough technical workers – be they developers, technicians or cyber pros – isn't likely to be solved easily, as the industry is one of many competing

for workers with these skills. And the shortage is affecting the potential growth for high-tech companies – a September 2021 Gartner study found that 64% of IT executives see the talent shortage as the most significant adoption barrier to emerging technologies.

And it's not just technical talent that's causing security industry challenges. Shortages of guards are commonplace among guard services companies and corporate security teams, and shortages in non-security industries like shipping, trucking and distribution are impacting the supply chain that industry firms depend upon.

PERSPECTIVES

"I've been through lots of different economic cycles. And what I'd say is in 2019 when we had really low unemployment – some cities across the country had 2 or 3% unemployment – it was hard to find people, but you could find people. Today, it is the most dysfunctional labor market I've ever seen."

– Steve Jones, Global Chairman and CEO, Allied Universal

"The issue is labor, and I think that's really going to hit us, not only in terms of us being able to find people to install, but people to manufacture. There's a huge labor gap right now that we're experiencing and we just can't get people in fast enough."

– Luis Orbegoso, SVP and President, Americas, Allegion

TECHNOLOGY SOLVING THE WORKFORCE CHALLENGE?

As Fredrik Nilsson noted to 2021 SNG attendees, "80% of the spending in the security industry today is manual labor That means guards, monitoring or even installation services." But Nilsson noted, "That will change." As automation and AI begin to replace manual work by some humans (even Allied Universal CEO Steve Jones noted that some of the corporate security data interpretation that formerly required human input is now being handled algorithmically), technology may lessen the dependency upon human workers, but no one expects those technologies to solve the workforce shortage problem quickly.

GREAT RESIGNATION

The much-touted "Great Resignation" of 2021, which left nearly 11 million jobs unfilled, was most impactful in the areas of technology and health care according to research published in the Harvard Business Review, with technology work resignations increasing by 4.5%.

Complicating the resignation trend and the overall workforce shortage is the fact that average salary increases were not expected to match 2021's inflation rates, according to the Society for Human Resource Management (SHRM).

And even as SHRM found pay rates that weren't keeping up with inflation, ADP Research Institute's data indicated that the average wage growth of someone who switched jobs in Q3 2021 was 6.6% – and that means workers are likely to continue to resign in favor of better-paying opportunities.

CONSEQUENCES OF CYBERSECURITY STAFF SHORTAGE

32% Misconfigured systems

30% Not enough time for proper risk assessment and management

29% Slow to patch critical systems

28% Oversights in process

27% Inability to remain aware of all

27% Rushed

Source: (ISC)² Cybersecurity Workforce Study (2021)

37% Percentage of SNG poll respondents who said that worker shortages would be the factor most likely to impact their business' ability to grow in 2022

60% Percentage of (ISC)² study participants in 2021 who indicated that a cybersecurity staffing shortage is placing their organization at risk

MEGATREND MOVEMENT

Workforce development last appeared in the 2020 Security Megatrends report, coming off 2019's extremely low unemployment rates. But amid the pandemic, as companies initially laid off workers and were challenged to put workers on customer sites, the issue briefly subsided and was temporarily removed from the Megatrends. For the 2022 report, workforce development came roaring back, as companies struggled to find installers and as labor shortages struck the entire supply chain.

TAKEAWAYS

FAST Foundation for Advancing Security Talent

Despite the enormity of the problem, moves are underway through organizations like the Foundation for Advancing Security Talent to spread the word of the industry's opportunities.

Labor and talent shortages are driving supply chain issues and even inflation in some sectors.

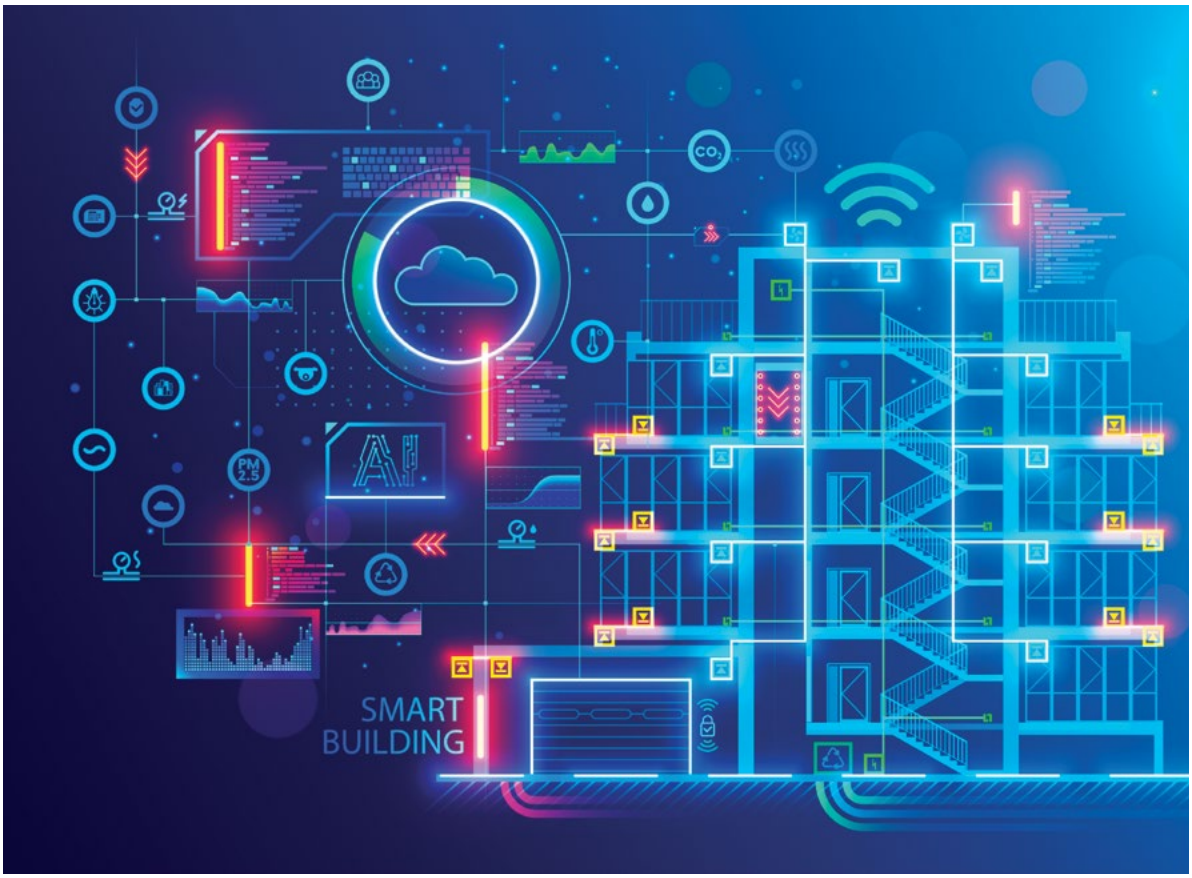
Promoting the industry as being open a diverse workforce can remove self-limiting hiring challenges.

Wage and benefits are likely to rise as companies compete for scarce talent.

Eventually, automation in some technology areas may reduce dependency on human workers.

MEGATREND 6

INCREASED INTEROPERABILITY



ASIDE FROM THOSE MANAGED by major corporate, institutional and government security users, the number of individual security systems that are integrated in the industry (such as between video and access control, or between the video system and the intrusion system) is still surprisingly low according to many systems integrators and manufacturers. That low rate of interconnectedness is changing, however, as more systems become open and as customers demand business operational insights and efficiencies that can only be determined by correlating data from multiple systems.

In the building environment, as in the security environment, the overall trend has been toward open systems or the use of common protocols that can allow communication between otherwise closed systems. With increased use of wireless technologies in the built environment and the network connected status of most control systems, advancing interoperability becomes more approachable, driving not only interconnected security platforms, but connecting security with other business systems.

THE INTEROPERABLE BUILDING

The common platforms integrated in a "smart building" type of environment include

- HVAC
- Security video
- Building access control
- Intrusion alarm systems
- Lighting
- Fire detection systems
- Mass notification systems
- Electrical power
- Elevator controls
- Parking controls

PERSPECTIVES

"Everyone wants to connect, and they want to be interconnected immediately, like yesterday."

– Michael McNeil, Chief Information Security Officer (CISO), McKesson Corporation

"We don't want things siloed separately. That doesn't really give us a clear picture of what we're dealing with. If we bring all these things together, and we've got our cameras, we've got our access control, we've got all of our monitoring technology, then we can tell what's happening at any given point in time in the airport. And that information is coming to us and we're not having to wait, or listen, or see, someone monitoring a screen all the time, or watching for an alarm to come to us."

– Megan Atkins Thoben, A.A.E., Director of Operations and Business Development, Louisville Regional Airport Authority

"Our buildings cost millions or even billions of dollars. They have the latest technology. But they don't know how many people are in them. They don't know when to turn the lights off or learn when to start warming or cooling office or meeting space. They don't reposition elevators for maximum efficiency, and they can't tell first responders where the fire is, where the medical emergency is, or what the quickest route up is. Nor can they tell occupants that the air is clean today, or that there's an elevated level of volatile organic compounds because the floors were just waxed yesterday."

– Journalist and author John Koetsier, writing for Forbes

"When you think about how you step into a building and the ecosystem that sits inside the building, whether that's the elevator system or the turnstile system or the visitor management system and the tenant amenity system platforms, we have to be able to be open in our ability to connect to all of those systems, to integrate with them, to be fully functioning inside that building. And every ecosystem will be different. And so, if you're closed off such that you cannot accommodate those, then your system will not work."

– Haniel Lynn, CEO, Kastle Systems

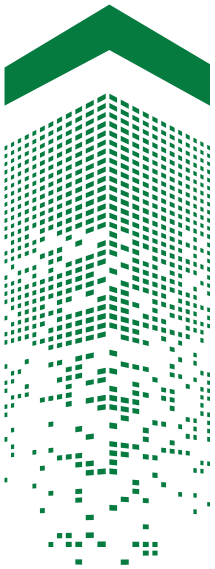
MORE BENEFITS, MORE RISK

One of the great clamors for interoperability is connecting physical security and IT systems with legacy operational technology and building systems. While McKesson Corporation CISO Michael McNeil says the demand for connection with these systems is high, it means more risk, because "most of those technologies in those types of environments are probably based on code that originally started back in the '80s."

$108B

Predicted 2030 global market value of the smart buildings IoT endpoint electronics and communications market, up from $55 billion in 2020

Source: Gartner Research



MEGATREND MOVEMENT

Increased interoperability as a singular trend may be new for the 2022 report, but it's not new to the industry. Retired from the 2022 Megatrend report were "Connectivity and the IoT of Everything" (trend #4 in 2021) and "Responsive Environments and Intelligent Spaces" (trend #8 in 2021), and both of these previous megatrends related to interoperability, whether among devices or systems.

TAKEAWAYS

Increased interoperability will require more standardization so that integration work does not require bespoke coding in most situations.

Connecting legacy building systems and OT systems brings increased risk due to legacy code bases of such systems.

Tremendous opportunity exists to simply connect disparate security systems, surprisingly few of which are commonly integrated.

MEGATREND 7

DATA PRIVACY

THE MEGATREND IS DATA PRIVACY, but underlying this trend is an overall increase of interest in individual privacy, particularly related to the public's concerns about how their data is being used and how they personally are being tracked, be it by security platforms, social media tools or even government systems.

The security industry, of course, is particularly relevant in that this industry's systems are often built to record data. Want to know who was in the building last night when the property was stolen? That's why video and access control systems exist. But with that power to collect data comes increased responsibility, and data can't simply be vacuumed up without processes and policies in place – particularly if it's data that captures individuals in environments within which they have a right to expect privacy.

This megatrend is being closely followed by legislators and regulators, and there are indications that data privacy will be more regulated by government in the future, with even some U.S. states considering or enacting their own legislation.

PERSPECTIVES

"[There is] entanglement of cyber and privacy as you can't have privacy unless you've got a secured container for all the PII. And if you're not guarding privacy, then what can you really say about the cybersecurity of your organization or your product?"

– Steve Van Till, President, Brivo

"Depending on where I have a camera, if I'm using it in a hospital or if I'm using it in a different environment, that could be considered privacy data as well. So, it's incumbent upon understanding where you're putting the product or device, what data it's generating and whether you've classified that and are saying yes, I consider this private data or privacy data, and I have to encrypt and also do things to protect it."

– Wayne Dorris, Cybersecurity Business Development Manager, Axis Communications

FIVE QUESTIONS TO ASK

1. Is it necessary to collect this information?
2. If yes, where should it be stored?
3. Who should have access to it and when?
4. Should this data ever be shared and why?
5. How long should the data be retained and how should it be safely disposed of?

For more prescriptive guidance, see SIA's guide to data privacy, "Putting Privacy Into Practice."

BREACHING NEW HEIGHTS

Loss of data privacy isn't always due to cybersecurity breaches but controlling data breaches is one way to protect your customers' data privacy. Unfortunately, according to the Identity Theft Resource Center, the number of publicly reported breaches that had been reported in the first three quarters of 2021 exceeded the total number of publicly reported breaches for the full year 2020.

GUIDING PRINCIPLES

Some 21 years ago, before data privacy was even in the lexicon of the security industry and long before GDPR was drafted or enacted, Richard Purcell was serving as the chief privacy officer for Microsoft, and in an article for Harvard Business Review, he set forth five guiding ethical principles for data privacy:

Notice: "Customers should receive full disclosure of who is collecting information about them, what is being collected, and for what purpose."

Choice: "Individuals should be allowed to choose how information will be used about them, how long that information will be retained, under what circumstances that information would be transferred to other parties, and so on.

Access: "We have to establish transparency by enabling customers to view, and even edit, the information we have so they can make sure it's accurate and relevant."

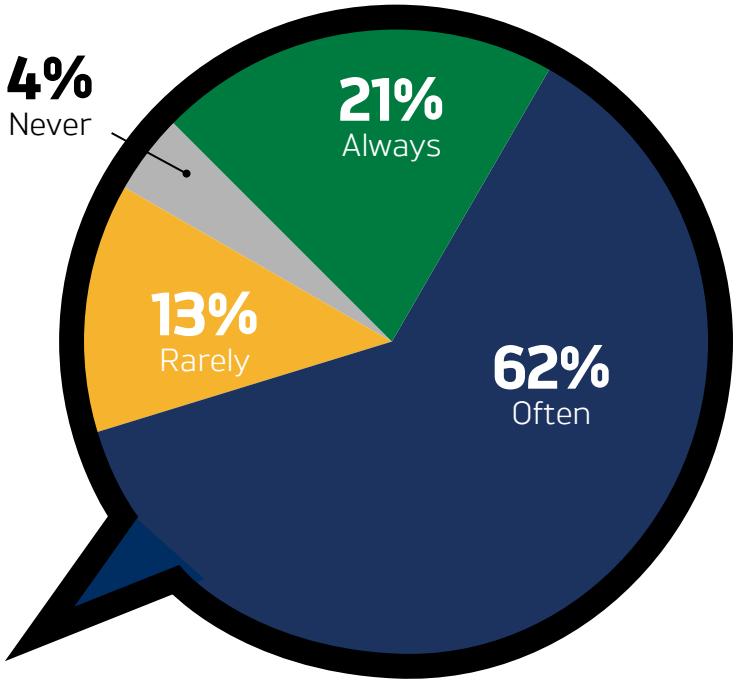
Security: "We must ensure that a customer's data are protected from unauthorized access, distribution, loss, or corruption."

Enforcement: "Some mechanism that will hold us accountable for complying with any stated policies. Third parties should be involved in maintaining that compliance."

SNG POLL

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

Data privacy conversations are occurring, but are they prevalent enough? A year ago, when we asked this same question, only 53% said that they "often" had these conversations with customers. Unfortunately, the growth in those conversations "often" occurring may be coming at the expense of those who previously said they "always" had such conversations, with that number dipping from 33% in the 2021 report to just 21% today.



MEGATREND MOVEMENT

Data privacy first appeared in the Security Megatrends in 2019 (ranked #6) and has stayed ranked continually since (#4 in 2020, #9 in 2021). This megatrend naturally links to technology trends like the adoption of facial recognition and other systems which can recognize and identify an individual.

TAKEAWAYS

Increased regulation and policy changes are likely to shape data privacy.

Companies need to define an individual or team that can develop and determine the company's data privacy policies.

Protection of private data requires a base layer of good cybersecurity.

MEGATREND 8

SECURITY AS PROPTECH

LOOSELY DEFINED, PROPTECH IS ANY TECHNOLOGY RELATED TO how buildings are managed or used, or even bought, sold or rented. And when it comes to how buildings are managed and used, security solutions – particularly building access control systems – are uniquely positioned to be one of the central data sources on building occupancy and usage efficiency. Security's position at the heart of the PropTech ecosystem is leading to renewed attention and increased valuations for security solutions companies that embrace the Proptech trend.

This megatrend, buzzword-laden as it may be, is about providing business insights for building owners, property managers and tenants. Security's mission changes from a role of preventing bad things to a mission of enablement: enabling great experiences for employees, enabling better property management, and enabling tenants and building owners to more efficiently use their space.

PERSPECTIVES

"[Security solutions] are the grandfather of all Proptech."

– Haniel Lynn, CEO, Kastle Systems

"The $100B Proptech revolution is providing a huge brand uplift for the security industry as more and more analysts appreciate that we are a foundational technology for the digital transformation of real estate."

– Steve Van Till, President and CEO, Brivo

"You're seeing changing expectations from building owners. It [security and building access control] was a utility and they wanted the cheapest solution that would last the longest without much maintenance. Today, the applications for that technology and the expectations of what they can do with that technology have changed."

– Lee Odess, General Manager of New Market Development, Latch

PROVIDING VALUE FOR OWNERS, MANAGERS AND TENANTS

Tenants, property managers and even building owners are finding direct value today from data coming out of the security systems, and the most referenced data is about occupancy. Tenants are using it to determine if they still need the same amount of space, or which office locations need more space or less space; owners and property managers are using it to track their financial performance and usage of shared tenant amenities. The data also is being connected to health conditions (see Megatrend 10).

Security solutions, chiefly access control, are also at the heart of the tenant experience. As a new wave of tenant experience platforms and apps have arrived from companies like Equiem, HqO and VTS, the one platform and app component that is always present is a connection to the access control system, because a great tenant experience starts with making sure the right people have the right access at the right time.

WHAT'S NEXT FOR SECURITY AS PROPTECH?

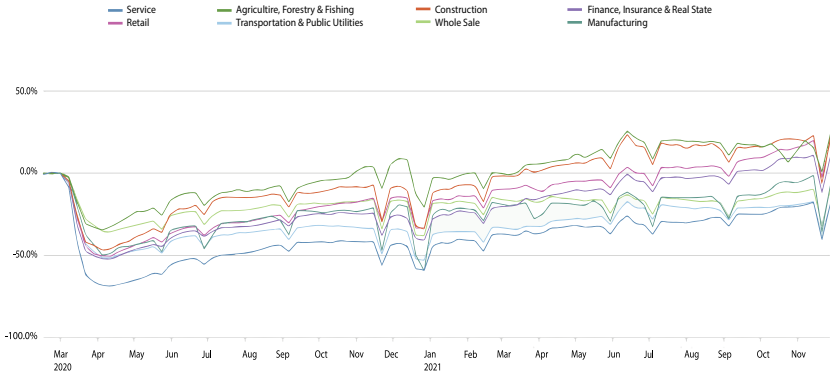
Experts expect more big-tech incursion, such as Apple's NFC credentials becoming a preferred identifying token. Third-party integrations will become even more common, particularly in the area of tenant experience apps. Data is likely to be aggregated across competing system providers and building operators to give urban planners more insights into how their cities are used. And on the business front, cloud-based access control companies may see higher valuations as they are seen fully as tech companies rather than purely security companies.

NOT JUST FOR A+

There's a common perception that Proptech is really just influential in Class A and A+ luxury office environments, but some property owners say that delivering Proptech solutions will make a Class B property tenant feel like they're receiving the Class A experience.

While initially viewed as a commercial real estate trend, Proptech is also providing data for multifamily residential properties like apartment complexes and condo towers, and at the individual residence level, Proptech is giving families insights into actions like a child arriving home from school, a package delivered or even status updates on home efficiency and comfort systems.

PERCENTAGE CHANGE IN DAILY ACTIVE USERS OF COMMERCIAL PROPERTIES BY INDUSTRY



Source: Brivo

$9.7B

Amount of new funding the Proptech sector attracted in the first half of 2021

Source: JLL 2021 Global Proptech Report

58%

Daily unique building access users compared to the pre-Covid daily average in February 2020 – an example of the level of data that access control solutions can provide.

Source: Brivo, data from Nov. 26, 2021

MEGATREND MOVEMENT

Newly ranked for 2022, this is nonetheless closely connected to the 2021 megatrend "Responsive Environments and Intelligent Space." This Proptech megatrend connects directly to the "Health & Sustainability" megatrend (Security Megatrend 10 for 2022), particularly as building owners and companies continue to navigate a return to the office.

TAKEAWAYS

Access control is at the heart of real estate property technology.

Security solutions companies, particularly those working in cloud-based access control, are seeing increased valuations and capitalization levels as the Proptech industry recognizes the value of such solutions beyond security.

The Proptech revolution and the approaches for how to use Proptech data are far from mature; new concepts for how to gain insights from Proptech data appear nearly daily, and industry players expect even more competition from big tech companies.

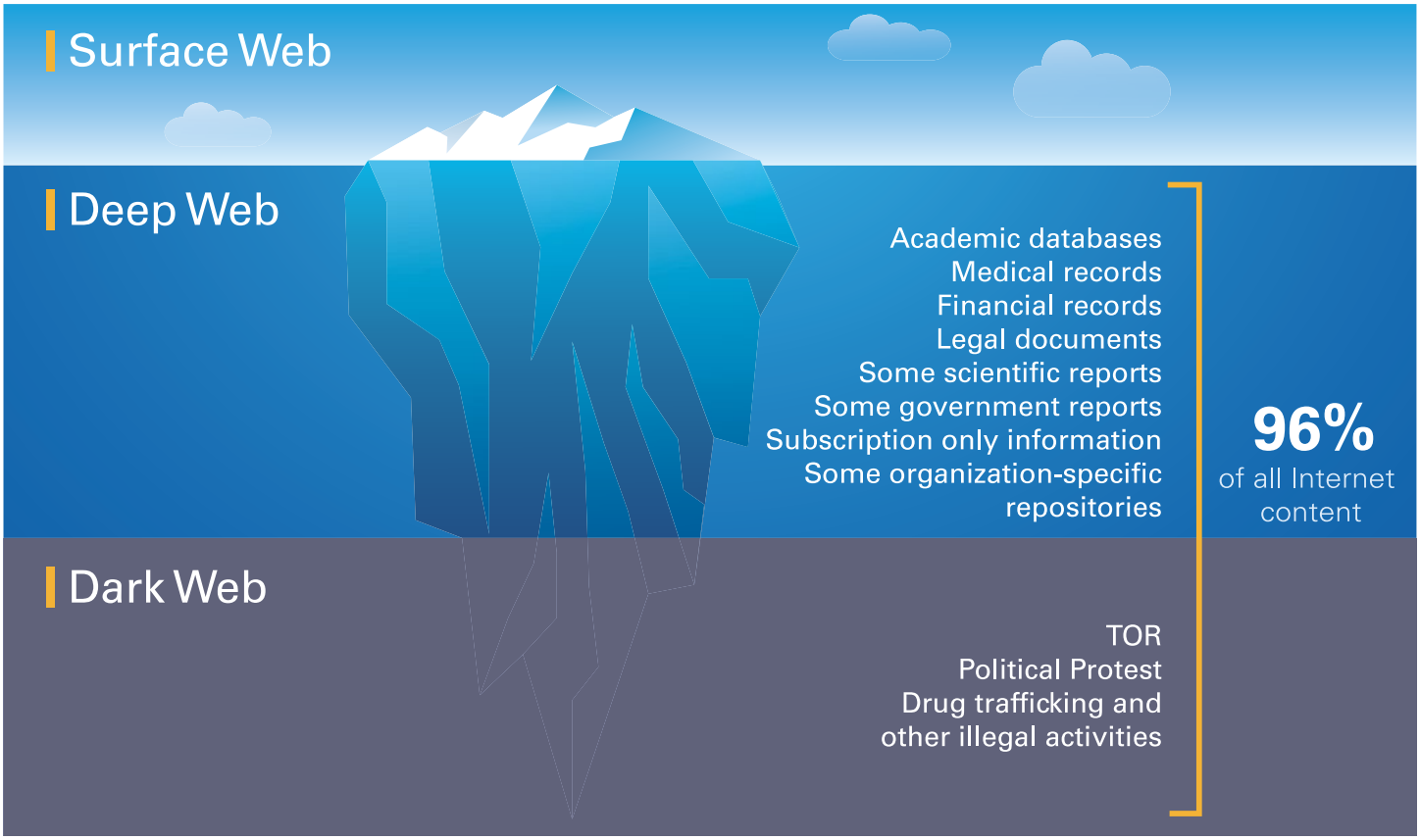
MEGATREND 9

EXPANDED INTELLIGENCE MONITORING

THE DATA YOUR CORPORATE SECURITY CLIENT WANTS is no longer limited to door alarms, card swipes and video footage. Chief security officers of the largest corporations today are seeking to mine intelligence from any public data sources that can give them an edge up in their security responses. Those intelligence sources could be social media feeds and posts that reference their brand or even their retail locations, but it's just as often public governmental data sources like U.S. Department of State informational feeds, weather data, international information related to disasters, terrorism and more. Beyond those public sources, companies are now scouring the dark web for potential threats, and all this information is now being processed and presented to savvy corporate security teams.

DEEPER AND DARKER

Expanding intelligence monitoring of public data sources on the surface web is already common, but companies and service providers are more regularly exploring reaches of the deep web and dark web to identify emerging threats or investigate stolen data.



MEGATREND MOVEMENT

Newly identified for 2022, this megatrend is as much a corporate security risk trend as it is a technological trend. It naturally relates to cybersecurity (No. 2) and data privacy (No. 7).

PERSPECTIVE

"On any one of these [social] channels, attackers might voice their intentions, spread false information concerning your organisation, or partake in more obscure but potentially equalling dangerous activities such as cyber-bullying or phishing. Because of the high number of users paired with the social nature of discussion, potential threats often emerge on these channels and forums first, even before they become a tangible risk."

– intelligence monitoring firm Signal

TAKEAWAYS

Corporate security leaders are looking to new intelligence sources to stay one step ahead of threats.

The dark web, where illicit data and content often resides, can be a resource for security executives seeking to understand emerging threats.

New firms are delivering intelligence-as-a-service, presenting the information in a coherent manner to security end users.

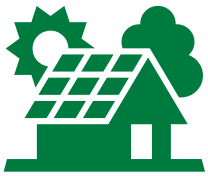
MEGATREND 10

HEALTH & SUSTAINABILITY

THE PANDEMIC LEFT AN INDELIBLE IMPRINT upon the security and safety industry, and while the initial response may have been to install security solutions that limited the need for touch or which could detect fevers, the conversation has expanded greatly from those early days. Our industry's role is the safety and security for people and places, so part of keeping people safe is being mindful of their health. And the second part of the conversation is whether these spaces and built environments able to sustain these occupants and if the components, devices and solutions going into these built environments are fundamentally sustainable themselves, including from an energy efficiency level. And by having these conversations and making these changes, can that make the security industry itself is more sustainable and thus more valuable?

INDUSTRY CONSIDERATIONS

- Contactless/touchless solutions
- Air quality and air control
- Detection of toxic chemicals
- Energy usage of all devices
- Minimization of material used in manufacturing and packaging
- Effect of entrances/door openings on building comfort and energy efficiency
- Interoperability with comfort systems (HVAC)
- Noise pollution
- Health-focused measurements: Contact tracing, occupant counting, mask wearing, social distancing



NOT JUST FOR COMMERCIAL

Research in 2020 by Parks Associates, and presented ESA and Resideo, indicates that consumer interest in health controls extends to the smart home, not just offices and business buildings. As the Parks Associates report notes, "The residential healthy home movement is an extension of the commercial green building movement."

PERSPECTIVES

"There's a lot of focus now on transparency and making sure that things that we're producing and that we're interacting with every day are healthy. We can provide not only sustainability goals in terms of how we make the things that we sell, but also what role they play in the building at large. For example, we want to reduce the amount of material in products. We want to reduce the amount of energy that they consume. And by doing that, it also has an outcome of positive effects in terms of delivery. If I am delivering smaller boxes that carry less weight, the carbon footprint is also reduced. And then of course, if I have openings that are more sustainably designed, that's going to reduce the amount of power; that's going to reduce the amount of emissions. It's going to have a really positive effect, even beyond the products that we make."

– Peter Boriskin, CTO, Americas, ASSA ABLOY

"As we started to see offices open up and employees coming in, whether it was full time or hybrid, we were seeing a greater involvement from real estate and workplace resources wanting to know how spaces were being utilized and the amount of time, for instance, people were congregating in a certain area, whether they were actually remaining at six foot distances from one another, and believe it or not, the amount of time they were standing versus seated."

– Henry Hoyne, CTO, Northland Controls

"We all want to minimize our carbon footprint and achieve that while now getting occupants back in a building safely with their heightened concerns."

– Joe Hudock, SVP Marketing and Sales Excellence, dormakaba

MEGATREND MOVEMENT

A new trend for the 2022 Security Megatrends report, Health & Sustainability is in some ways the evolution of the 2021 report's named trend of "touchless & frictionless solutions," which was ranked #6 in last year's report.

TAKEAWAYS

The COVID-19 pandemic created an awareness of how security solutions can be used to protect the health of employees, visitors and customers.

Leading manufacturers are considering the sustainability of the solutions they deliver, from how much energy they draw to even if devices can be made with less material or packaged more efficiently.

Driving increases in health and sustainability, particularly in building environments, will require expanded interoperability.

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