WINTER 2023 SPA ISSUE 23.1

The SECURITY Advisor

a magazine published by Security ProAdvisors for the Security Industry

PRESIDENT'S CORNER

Hello and welcome to the latest edition of The Security Advisor.

Perhaps no issues are more paramount in the security field today than the needs for both robust cybersecurity defenses, and the integration of those defenses with an organization's physical security infrastructure. Those needs are not going away - in fact, they are ever-increasing - given the evolution of technological systems, the continuation of at least some remote work situations, and the constant attempts at intrusions into company business by bad actors.

That's all underscored by the *Security Industry Association's* placement of the *"Cybersecurity of Physical Security"* at the top of its Megatrend list for 2023. *"Security has truly converged, whether we think it has or not,"* SIA notes, adding that wise buyers of security devices are asking pointed questions about the risks those interconnected devices pose, and wise integrators and solution vendors are ready with credible and comprehensive answers.

"Cybersecurity has to be managed on multiple levels, requiring constantly expanding investments" on several fronts, the *Megatrends* report notes. These include on-site devices like cameras and readers, infrastructure like wiring and networks, software and servers, the cloud, mobile devices like phones and tables, and last but not least, users themselves - who are vulnerable to social engineering attacks, or, conversely, can pose insider threats.

The *SIA* poses three options for security practitioners in facing this picture: ignore it entirely, which most deem unwise; keep teams in separate but equal channels while ensuring open dialogue and cross-investigation, which can work but might not be optimal; or go fully converged, which is probably the best defense against *"converged threat vectors that impact information, data, people and assets,"* the report says.

This edition of The Security Advisor features a Q-and-A interview with a security professional who thoroughly understands and appreciates the importance of these principles, as do we, and has brought his organization to the seamless leading edge of what *SIA* recommends - which made him an easy choice for us to want to interview.

Shawn Henry, a former FBI agent, now serves as chief security officer with global technology services company *CrowdStrike*, which provides services for an impressive array of Fortune 500 and international companies in verticals ranging from hospitality, to manufacturing, to critical infrastructure.

Mr. Henry told us about the evolution of security challenges during and after the height of the pandemic, how the ever-tightening convergence of physical and cybersecurity is impacting his company and others, how he's been pursuing closer collaboration with law enforcement, and the latest and greatest in employee training to ensure continued success.

As has been our custom, we also detail the latest in mergers-and-acquisitions activity in the security space over the past six months, which has been rather busy to say the least. This has included *State Farm's* purchase of a 15% equity share in *ADT, Protos Security's* acquisitions of *MG Security* and *Blue Star Security, Allied Universal's* buying of *Century Event Security & Staffing, GardaWorld's* purchase of *ARCA, Sesami's* acquisition of *planfocus, PalAmerican's* buying of *ProTech, Motorola Solutions'* acquisition of *Rave Mobile Safety, NRG Energy's* purchase of *Vivint Smart Home, Sting Alarm's* buying of *Signal Fire*, and *Prosegur Cash's* acquisition of a controlling stake in *ChangeGroup.*

These M-and-A's and others to come as 2023 unfolds are happening against a backdrop that's not unlike conditions throughout last year. Labor markets continue to be tight, with hiring of personnel an ongoing challenge. Inflation has eased somewhat from the spikes of a year ago, but it's still considerably higher than the decades-long norm. Interest rates are also higher than at any time in recent memory as the *Federal Reserve* continues to boost them, albeit more modestly, to ensure inflation continues to cool. Yet despite all of those headwinds, valuations in the security space remain robust - probably because the demand for security remains extremely strong. As the recent tragedy at *Michigan State University* underscores, threats - whether cyber or physical - can come at any time, without warning, and we all must stand at the ready to protect and serve on either front.

Keith Oringer
Founder and President
Security ProAdvisors

SECURITY ProAdvisors
THE SECURITY ADVISOR

Published twice a year, The Security Advisor is a magazine dedicated to news in the security industry throughout the world. The Security Advisor is published by Security ProAdvisors, providing advisory, consulting, and brokerage services to the security industry - guarding, system integration, and electronic security. Security ProAdvisors represents sellers in security transactions.
www.SecurityProAdvisors.com

HEADLINES - M & A

State Farm Purchases 15% of ADT

Insurance company *State Farm* has purchased a 15% equity share in *ADT* with a $1.2 billion investment, including up to $300 million to finance product and technology innovation, customer growth and marketing.

To hone its ability to optimally monitor, detect and prevent risks to homeowners, *ADT* will both partner with *State Farm* and further build its relationship with *Google* with the goal of finding the mix of state-of-the-art security, smart home technology and risk-mitigation capabilities. *Google* has separately agreed to commit another $150 million, boosting its total commitment to $300 million, as long as *ADT* hits specific milestones.

In creating this comprehensive solution bridging home and mobile safety, *ADT* says customer benefits could include safe homeowner discounts that lower *State Farm's* insurance premiums for those that employ *ADT's* smart home security systems based on *Google's* devices. The partners believe lowered risks from *ADT's* patented SMART monitoring technology for events like water or fire damage, or home intrusion, will lead to fewer and less severe claims.

"ADT's partnership with State Farm creates the capability to drive innovation in homeowners' insurance on a broad scale. By delivering a truly connected home, together we can improve the customer experience and provide more peace of mind," said Jim DeVries, *ADT* president and CEO.

"This partnership gives State Farm the opportunity to provide smart home technology that takes us from our 'repair and replace' model to a 'predict and prevent' mindset," said Paul Smith, executive vice president and chief operating officer of *State Farm*, who will take a seat on *ADT's* board of directors as part of the arrangement. *"These innovations will help us take the next step into the future of home insurance and add more value for our customers."*

Protos Security Acquires MG Security, Blue Star Security

Security Services Holdings - which does business as *Protos Security* and is a portfolio company of *Southfield Capital* - has acquired both *MG Security Services*, to boost its presence along the East Coast; and *Blue Star Security,* to do the same in the Midwest.

The New York City-based *MG Security*, which employs more than 1,200 guards, provides such services as both armed and unarmed security guards, crisis management, fraud prevention and private investigation in vertical markets like hospitals, education, financial services, property management and commercial real estate.

"*MG Security Services* is *a highly reputable security and risk mitigation firm with unmatched experience and credentials. This acquisition greatly accelerates the growth of our organization and enhances our service offering in the NYC Metro area while also positioning us as the fourth largest security services provider nationally,*" said Anthony Escamilla, chief financial officer at *Protos Security*.

Manny Gomez, founder and president of *MG Security Services*, who will join the leadership team at *Protos*, added: "*We are excited for our new partnership with Protos. The combination of our tenured management team and extensive experience in law enforcement, including NYPD and FBI, will provide enhanced service offerings to clients."*

continued on next page...

HEADLINES - M & A
continued

The ***Protos*** purchase of Chicago-based ***Blue Star***, which provides armed security through more than 850 off-duty and retired law enforcement officers, gives the company an expanded presence in Illinois, Indiana and Wisconsin among both Fortune 500 firms and small to medium-sized businesses.

"This strategic acquisition further strengthens our service offering and we look forward to providing our customers with an enhanced suite of security solutions, particularly as it relates to off-duty police officers," Escamilla said. "Our ability to provide a holistic set of security solutions to meet all customer needs continues to improve and adding ***Blue Star Security*** *to the Protos family positions us well for continued growth."*

Added Jeffrey Salvetti, co-founder of ***Blue Star,*** *who will join the leadership team of* ***Protos*** *along with co-founder Anthony Varchetto: "****Protos*** *shares the same values of consistency and professionalism, and it was clear that this partnership was destined to be. We believe our service offering will be highly complementary as we drive growth and create value for new and current customers."*

Allied Buys Century Event Security & Staffing

Allied Universal has continued its buying spree of recent months and years by adding Orlando-based ***Century Event Security & Staffing***, which handles the full spate of security and event services in top exhibition industry cities Orlando and Las Vegas with several thousand employees.

"This important acquisition, a first for our event services business, aligns with our strategic growth strategy by providing additional operations and qualified staff in two of the nation's most prominent cities for exhibitions and events," said Steve Jones, global chairman and CEO at ***Allied****, which gobbled up 10 companies during the first half of 2022 and 10 others in 2021, including* ***G4S****.*

Added Marty Stein, ***Century Event Security & Staffing*** *chief financial officer: "Becoming part of an organization with the resources, technology and depth of service that* ***Allied Universal*** *offers enables us to continue providing even more value to the customers and communities we serve in the event services market space."*

Motorola Solutions Acquires Rave Mobile Safety

Motorola Solutions has acquired Framingham, Massachusetts-based ***Rave Mobile Safety,*** which offers mass notification and incident management that enables communication and collaboration during emergencies. Terms of the deal were not disclosed.

The platform allows for more effective communication of health emergencies, lockdowns, evacuations and other operational updates and alerts, so those affected are more aware of what they need to do. ***Rave's*** clients include organizations and public safety agencies such as hospitals, higher education institutions, K-12 school districts, and state and local governments.

The platform will be integrated into the technology portfolio already offered by ***Motorola Solutions***, which incorporates such features as access control, video security, body cameras, critical communications, command center software, and weapons detection solutions.

*"****Motorola Solutions****' technologies strengthen the critical intersection of public safety and personal security," says Greg Brown, chairman and CEO,* ***Motorola Solutions****. "Our acquisition of* ***Rave*** *complements our portfolio with a platform specifically designed to help individuals, businesses and public safety agencies work together in more powerful ways."*

*"****Rave and Motorola Solutions*** *share a deep understanding of communication and collaboration workflows for customers, including the essential role of mobile technology, when addressing complex and evolving safety challenges," says Todd Piett, CEO,* ***Rave Mobile Safety****. "We're excited to extend our reach and impact as we join a global leader in public safety and enterprise security."*

HEADLINES - M & A

GardaWorld Purchases ARCA, Subsidiary Sesami Acquires planfocus

Montreal-based *GardaWorld* has purchased cash technology solutions firm *ARCA*, completing the guarding behemoth's 10th deal of 2022 and bringing total acquisitions to more than $1.3 billion year-to-date.

The company and its 320 employees will become part of global cash ecosystem integrator *Sesami Cash Management Technologies*, which operates as an independent entity of *GardaWorld*, which also announced it has reached agreement with the provincial government of Quebec for a $300 million strategic investment through Investissement Quebec, via a private placement of *GardaWorld* preferred shares.

"The strategic investment enables GardaWorld to acquire high-quality companies like ARCA, and to keep innovating and leading the industry," said Stephan Cretier, CEO of GardaWorld.

Meantime, *Sesami* has separately acquired global financial technology software company *planfocus*, a nearly two-decade-old Munich, Germany-based firm that offers cash optimization software solutions aimed at reducing logistics spending and cash holding costs, while boosting client service levels and availabilities.

Sesami's integration of *planfocus*, which optimizes the operations of more than 78,000 bank branches, ATMs and cash processing centers and moves more than 300 billion Euros in physical cash shipments annually, widens the international client portfolio of *Sesami* - an independent entity of *Garda World Security Corporation* - with additional financial institutions and consumer businesses, while providing its existing client base expanded cash optimization services.

"With this acquisition, Sesami becomes the global leader in cash optimization solutions, with an unrivalled technology stack now up-scaled with the addition of planfocus' cutting-edge cash optimization software," said Steph Gonthier, CEO of Sesami. "Integrated to our enterprise cash ecosystem software platform, planfocus' AI based technology and strong team will further enable Sesami to deliver the only true end-to-end tech-enabled cash ecosystem solution to financial institutions and consumer businesses."

"We are extremely proud to be joining forces with Sesami, a state-of-the-art innovator and disruptive global leader, to offer a true end-to-end and fully integrated cash software solution enabling financial institutions and consumer businesses to seamlessly manage and outsource their entire cash ecosystem," said Dr. Joachim Walser, CEO and co-founder of planfocus.

"As part of Sesami, we will now be able to truly scale our next generation technology and bring our unmatched cash optimization solutions to a broader global client base."

PalAmerican Buys ProTech

PalAmerican Security has bought San Francisco-based *ProTech Security*, adding more than 700 employees, two new offices in San Francisco and Oakland, and a sizable portfolio of office towers to *PalAmerican's* stable.

The 28-year-old *ProTech* has provided security throughout the San Francisco Bay Area, becoming one of the larger regional security services providers, and the acquisition will deepen *PalAmerican's* ties to northern California and the West Coast.

"This is a very exciting acquisition for PalAmerican Security," said Jason Begin, president of PalAmerican Security. "We are eager to expand our operations in San Francisco and Oakland, while continuing to grow our presence in California."

"Our plan is to invest more resources into our new operations to better serve our clients while offering tremendous growth and advancement opportunities for the people within our company," added Ashley Cooper, CEO of PalAmerican Security.

Q&A with Shawn Henry, CrowdStrike

Shawn Henry serves as chief security officer for CrowdStrike, a global cybersecurity company that works with nearly half of the Fortune 500 and some of the largest entities globally in areas like transportation, technology, hospitality, manufacturing, critical infrastructure and the public sector.

A former FBI agent, Mr. Henry retired in 2012 from the bureau's senior executive service as executive assistant director, where he oversaw half of the FBI's investigative operations. Now, he supervises all aspects of security for CrowdStrike, ranging from the physical security of its global facilities, personnel, executives and events, to the company's information security, business continuity and resiliency, and risk reduction programs.

We talked with Mr. Henry about the security challenges his company faces as the pandemic wanes and physical-cyber security convergence continues to ramp up. We also asked him about the need for greater collaboration with law enforcement and more comprehensive training for employees.

Keith Oringer: *What are some of the unique security challenges facing a global technology services company like CrowdStrike?*

Shawn Henry: We're a security technology company that protects some of the biggest companies around the world from many different cyber threat actors that are seeking opportunities to get inside organizations, such as nation-state actors like Russia, China, Iran and North Korea, and organized crime groups. There's no shortage of adversaries looking to steal information or to disrupt those networks, and they've got very substantial capabilities. Trying to stay a step ahead of the adversaries, while constantly innovating our solutions, maintaining a high level of rigor and our sense of commitment and mission to protect our customers - it's all a challenge. And we're very, very fortunate to have amazing employees in the organization who are focused on the mission: stopping breaches.

CROWDSTRIKE

KO: *How has the COVID-19 pandemic impacted CrowdStrike's physical and cyber-security operations over the past 2 1/2 years?*

SH: We were built as a remote-first company. Before COVID, about 70% of our workforce was remote already, so when the pandemic hit, it wasn't a major impact on us to move people off-site. Our technology, as a cloud-based security company, is built for that specific purpose. What the pandemic did do, though, was offer us a lot more opportunities - because as corporations moved to the cloud and made their workforces remote, they did not necessarily have the capabilities in place to secure their new infrastructure. As a result, we were really pressed into action. Because of that significant increase in workload, we had to scale to meet the demand by growing our workforce, which, from a security perspective, resulted in increased background investigations, a lengthy vetting process, and the onboarding piece. That was a lot of extra work for us, but it was done for the right reasons: to support the increasing remote workforce of these global corporations. It was an interesting couple of years.

We're in a really strong place now, and a lot more companies have adopted our remote-first workforce model. I think they've learned that it's easier for them to recruit people. In many cases, they're more effective and more efficient. I think that we'll see that model continue long-term.

continued on next page...

Q&A with Shawn Henry, CrowdStrike
continued

KO: *It's interesting, you hear about some companies whose top executives have a different mindset. They want to have control, and some people are now coming back into the buildings in New York.*

SH: That's important. There are parts of our organization where there are some synergies by having people together because of very quickly changing adversary models and the ability to share intelligence. When people are training, for example, oftentimes, it's easier when you're sitting next to somebody than doing it over Zoom. There's pros and cons, always. So, I think every company needs to determine what the right mix is for them. There are so many considerations in addition to the efficiencies. You've got to look at the costs, you've got to look at morale, you've got to look at the retention and recruiting that I mentioned earlier. Each company has to make that determination, but the fact is that remote workforces and cloud-based capabilities are not going away.

KO: *Given your responsibilities, and the increasing pace of technology convergence, how does CrowdStrike approach collaboration between physical and IT security?*

SH: It's a really important question. I've said for the last few years that there are more similarities between the physical world and the IT world than there are differences. There's this merging of the two worlds. Historically, people have looked at information technology as this kind of ephemeral, up-in-the-ether type of delivery system. But the reality is, there's a lot of physical components to digital: there's hardware, data centers, people operating pieces of equipment. There's always going to be that link. In our organization, I'm the chief security officer, and I've got information security in my area of responsibility, as well as the physical security of our buildings and our people. It all comes within the same chain of command. And I think there's a lot of value there because of the sharing of intelligence, and the ability to collaborate.

I talk to a lot of companies, and they've got the chief information security officer reporting to the CIO; they've got the physical security people reporting to somebody else - maybe the CEO, or the CFO, or the general counsel. And sometimes there's this deep bifurcation that inhibits collaboration and creates blind spots for companies from a security perspective. The ability to work in a collaborative environment, to share intelligence across all risks to the company, physical and digital, is the right model. Many companies have different iterations of it, and you've got to do what's right for you; but at the very least, there needs to be an absolute coordination and sharing of intelligence between the two teams, even if they're not the same chain of command.

KO: *Right, you can react a lot quicker if it's under one roof rather than two. And then you don't get into the politics, with everyone controlling their domain or their power base.*

SH: I'll give you a great example. You have a company that has an insider threat of a disgruntled employee, who is now exfiltrating data from the internal network because they're going to go to a competitor. If you're on the security team, and you've got a physical human being who's sitting in an office or working from home; you've got one security group that's responsible for disrupting that employee, or for exiting that person from the organization. You've got a whole other group of people who are responsible for looking at what has been exfiltrated, or somehow engaged in the collection of evidence. You also have a team responsible in case the disgruntled employee deploys some type of malware in the environment. It would be wonderful if people are not only talking to each other, able to move at the speed of the internet and not have to wait for somebody to make a decision, or for another supervisor to sign off on documentation - but also reacting in real time to get ahead of some of these things.

KO: In this post-pandemic work world, what are your concerns about CrowdStrike employees using internet-connected devices for business outside of the office?

SH: My answer is always: it depends. Every company is going to be a little different. You've got to allow employees to utilize their work resources for what we would call - going back to my time in the government - de minimis use for personal work. Somebody wants to check their personal email account, or they're having a text-chat with their parents about a big party coming up over the weekend, that's de minimis use. I had a big meeting last week with about 15 CISOs, and we were talking about companies that have found employees working multiple jobs in the remote workforce. Somebody who's literally sitting with two computers, getting paid two salaries, and working on two computers for two separate companies at the same time. That, of course, would be completely inappropriate and unacceptable - quite honestly, that's fraud.

continued on next page...

Q&A with Shawn Henry, CrowdStrike
continued

We've got to build an environment that allows our employees to engage in some private activity, but we've got to also instill in them a sense of responsibility. You're not spending three hours a day on some separate side project, or you're not engaged in outside employment that's impacting your ability to do your job. It's incumbent upon the employees, it's incumbent upon the managers, it's incumbent upon the company to ensure that the parameters are very clearly described and enforced. And that's what we do here. We make sure that folks are well aware of what the protocols are, and what acceptable behaviors are.

KO: *What advice do you have for CSOs and CIOs in working with organizations to add new physical and IT security tools and technology?*

SH: I talk to boards all the time about risk, and what the impact might be on the company to have some type of an exposure of data or disruption of their network. And it's really important for these companies to ensure that they've got cutting-edge technology that allows them to keep up with the pace of innovation. I mentioned at the outset the sophistication of the adversaries that we deal with—if you don't have the proper tools to identify their anomalous behavior, you're not going to even know they're on your network. You've got to invest in technology, both on the physical and the IT side, because the risk of not doing so is so high. If you're unable to detect or see anomalous behavior, the first time you're going to know there was a problem is after something bad has already happened.

You need to have the right capabilities from a physical perspective, access to intelligence sources, access to technology that allows you to lawfully look at unusual behavior, and access to IT security tools and technology that allows you to detect these types of activities before they create that negative impact. You've got to stay abreast of that. And I know a lot of CISOs and CSOs that are talking to their peers regularly, looking for best practices, looking for recommendations on new technology. That's also an important part of the CISO or CSO job, is making sure you're staying tuned in to what the current behaviors or trends are, and where there's opportunity to make yourself more effective and more efficient.

KO: *How do you go about promoting a company-wide security culture, and how do you see that challenge evolving?*

SH: It's the tone at the top - it all starts with leadership. If the leader doesn't think something's important, the rest of the company is not going to think it's important. I talk to boards and C-suites all the time about the need to lead from the front, to lead by example, to carry the right message, and to set that tone. In our company, we have a security-first mindset that is instilled from the very day people onboard as a new hire. It's one of the first things that they hear from me, personally, about understanding what the risks are and recognizing the role that individuals play in defending the company. I talked a minute ago about the tools and technology that you need, but it starts with people. It starts with people having a recognition of what the risks are, and then understanding their role as a first responder - seeing something and saying something.

If you see something unusual - somebody walking in, they don't badge-in, but they walk in behind somebody else - challenge them. Or you get a phishing email that has some type of a malicious payload on it, and you're trained to recognize those things, you alert the CISO so that they can pull it out of everybody else's mailbox. Those are little things, but it's about building that culture. And culture is important. We have a very strong culture in our company. I send out messages regularly, our CEO talks about it regularly, and it's addressed when we do our all-hands communications. We do a lot of testing, internally, of our employees so that they recognize the risks. And people who violate those rules - certainly, if they do it willfully - we ensure that there are consequences. Otherwise, it's more of a suggestion than a deterrent.

continued on next page...

Q&A with Shawn Henry, CrowdStrike
continued

KO *Given your professional background, how do you approach collaboration between CrowdStrike and law enforcement agencies?*

SH: First off, I'm a big believer in collaboration, not just with law enforcement agencies, but with other companies. We've been very collaborative with some of our competitors, where we found something that was unusual, and we shared it with them, so they could share with their customers. Recognizing that our competition is less important than getting out the message and helping to secure infrastructure. Collaboration is very, very important. We've got a lot of partnerships in this industry.

I've encouraged companies to share with law enforcement. I can't do it unilaterally without their concurrence, but I've many times suggested: "Look, here's something that the FBI or the Secret Service could use. It's valuable intelligence. We can share it in a way that does not undermine you, or place you at risk, but it would be helpful for the broader internet community." And that works well and has resulted in some really positive interactions.

My background allows me to have conversations with law enforcement because I understand what they're trying to do, and what they need to accomplish their goals. And again, I can oftentimes navigate between the victim-customer and law enforcement in a way that allows for a win-win situation. Law enforcement is able to get what they need, and the customer maintains their privacy and is not put at greater risk. And that's helpful for all parties involved.

KO: How do you see your approach to security training and awareness evolving, especially as a global company?

SH: Awareness has really got to be top of mind. I'm still bumping into executives of major companies who do not have an appreciation for their risk, and I take that seriously. Organizations need to understand what they're facing. They have the ability to influence the long-term success of their company; conversely, they also have the opportunity to negatively impact their company because of a lack of attention, or a reluctance, or malfeasance. If they're not paying attention, if they're not aware of the risks, they're putting themselves, their customers, and their employees at risk.

Internally, every company needs to ensure that they've got an adequate training program in place. We've seen in the physical world companies doing active shooter drills and of course fire drills. Those are normal courses of business; fire drills have been for many decades, active shooter drills in the last five years or so. There needs to be drills and training around cyberattacks, and companies need to adopt that. They need to encourage it. They need to hold people accountable if they're not taking the training, because awareness is the first piece in a successful defense.

KO: *With all the lessons learned over the course of your career, what's your best piece of advice for security professionals?*

SH: There are a couple of things. First of all, you can never become complacent. You've always got to be on edge. People tell me I'm intense. And I feel good about that [description] because I don't ever want to be asleep at the switch. You want to be looking forward, to see what's coming through the windshield. You don't want to be looking in the rearview mirror to try to figure out what just hit you. The other piece that's really important for security professionals, is to position yourself in your company as an enabler of the business. Too often, people see security as an obstacle: "No, the CISO doesn't want us to do this, the head of security doesn't want us to do that."

If people understand the risks, they're going to be more accepting and more willing to take actions. Because rather than being told, "you can't do this," if they understand why they can't do it, it helps them to have a better appreciation. If you want to be an enabler of the business, you've got to make allies within the organization. The general counsel can be one of your biggest allies: somebody who has an appreciation for risk, somebody who can help represent to others who might not understand what the corporate liability is, what the regulations are related to HIPAA, for example, or PCI (payment card industry). They can help you spread that message.

It's about developing relationships and getting people to buy into what you want to do, not you walking around with a big stick telling people they have to do things. It's about you encouraging people. They want to do it because they respect and appreciate you. They want to do it because it's the right thing to do. Not because that crazy guy in the corner office told us we had to do it.

HEADLINES

NRG Energy Purchases Vivint Smart Home

NRG Energy Inc. has purchased Provo, Utah-based *Vivint Smart Home, Inc*., for a total of $5.2 billion, including $2.8 billion in cash - or $12 per share - along with the assumption of $2.4 billion in debt.

NRG, a Fortune 500 company, provides electricity, natural gas and other energy solutions to millions of people and organizations. *Vivint Smart Home* provides technology, products and services aimed to provide a smarter, more efficient and safer home to nearly 2 million customers, combining multiple devices into a single platform that leverages artificial intelligence and machine learning.

*"The acquisition of **Vivint** is a transformational step in achieving our vision," said Mauricio Gutierrez, president and CEO of **NRG**. Customers want simple, connected, and customized experiences that provide peace of mind. **Vivint's** smart home technology strengthens our retail platform, improves our customer experience, and increases customer lifetime value."*

*"Our agreement with **NRG** is the culmination of our board's ongoing pursuit of maximizing value for Vivint stockholders and is a testament to the strength of the Vivint brand, capabilities, and proven industry leadership," said David Bywater, CEO of **Vivint Smart Home**. "We look forward to working with **NRG** to create exciting opportunities for **Vivint** as part of a larger platform."*

Palantir, Crisis 24 Announce AI-Oriented Partnership

Operating systems builder *Palantir Technologies Inc.* and integrated risk management firm *Crisis24*, a *GardaWorld* company, have formed a multi-million dollar, long-term strategic partnership aimed to *"transform security and risk management with the power of AI,"* the two companies have announced.

The partnership expects to *"provide clients with innovative solutions [and] data-driven insights for results-oriented decision-making that meet their everyday challenges,"* according to a press release. The combination of AI and human insights will help to pinpoint trends in risk as they first become apparent, enabling *Crisis 24* to provide up-to-the-minute and specifically targeted insights to its clients, improving their resiliency.

*"Every organization must be able to understand, anticipate and react effectively to risks as they evolve," said Alex Karp, co-founder and chief executive officer of **Palantir Technologies.** "This requires leveraging the massive amount of relevant data out there and distilling it down to usable insights."*

*"This strategic partnership is a paradigm shift in the delivery of security risk intelligence. It will allow **Crisis24** to conquer new frontiers as the most powerful and advanced source of risk intelligence and analytics in the world," said Stephan Crétier, founder, president, and CEO of **GardaWorld and Crisis24**.*

HEADLINES

EQT Partners Invests $1.4B in Top Korean Firm

Swedish investment giant *EQT Partners AB* has invested more than 2 trillion won (about $1.4 billion) to purchase a 36.87% stake in *SK Shieldus Co.*, the second-largest physical security firm in South Korea, from a consortium led by *Macquarie Korea Asset Management*, according to the *Korea Economic Daily*.

While completing its first transaction in Korea since opening a Seoul office in January 2022, which could make it the largest shareholder in *SK Shieldus, EQT Partners* is also in separate talks to purchase equities of *SK Shieldus* from Korean investment manager *SK Square Co., EQT's* largest shareholder, with a 63.13% stake.

Littlejohn & Co. Invests in The Hiller Companies

Littlejohn & Co., a Greenwich, Connecticut-based investor in middle-market companies, has invested in fire and life safety product and service provider *The Hiller Companies*, acquired 10 years ago by Netherlands-based multinational *Pon Holdings*, which will maintain an equity stake, according to *Private Equity Professional*.

On the service side, *Hiller* offers design, engineering, inspections and maintenance for fire suppression, detection and sprinkler systems; while in terms of products, it provides portable and fixed fire extinguishers, hoses and reels, nozzles, foam and other equipment, as well as gloves, fire resistant clothing, safety glasses, masks and air-breathing apparatuses.

"Littlejohn has a demonstrated track record of scaling businesses in the facility services sector, and I am excited to partner with them as we seek to expand our capabilities while continuing to deliver for our customers," said Jeff Birch, CEO of the century-plus-old, Mobile, Alabama-based Hiller. "We look forward to leveraging the firm's resources to accelerate our growth trajectory and execute the meaningful organic and inorganic growth initiatives available to our company."

Securitas Grows Sales 6%, Operating Margin Hits 5.8% in First Nine Months of '22

Securitas reported total sales of 95.1 billion Swedish Krona for the first nine months of 2022, or about $9.15 billion, up 6% year-over-year. Operating income was about $533 million, while operating margin was 5.8%, the company reported. Earnings per share reached $6.4 million, while net debt/EBITDA was 5.8.

President and CEO Magnus Ahlqvist noted that the third quarter of 2022 marked the first one that *Securitas* had absorbed the acquisition of *STANLEY Security*, concluded on July 2022, which helped spark organic sales growth of 7% in that quarter alone.

"Our investments in a stronger client offering are generating results with good commercial traction," he remarked. "We recently also renewed a significant global contract with expanded scope of services, reaffirming our position as the leading security solutions partner to many of the most well-known brands worldwide."

Ahlqvist said the expects synergies to continue to blossom in the wake of the STANLEY acquisition. "Bringing together our two great companies gives us a leading position in the industry," he said. "Combining our talent and expertise sets us up for stronger growth thanks to an outstanding client offering and we expect significant margin enhancement opportunities going forward. Together we have great potential to provide tech-enabled security solutions that create long-term value for our clients and shareholders."