IDC ANALYZE THE FUTURE

IDC MARKET SPOTLIGHT

Sponsored by: Security Industry Association

Digital technology is reshaping industries and operations and has extended into the realm of security technology. Modern technologies such as robotics, drones, and artificial intelligence are enhancing the capabilities of security officers, but procurement presents new challenges and demands a unique approach.

Next-Generation Security Technology Requires a Strategic Approach to Procurement

June 2019

Written by: John Santagate, Research Director, Service Robots

Introduction: Technology Evolution Is Disrupting and Enhancing Security

AT A GLANCE

KEY TAKEAWAY

As next-generation security technology evolves and use case opportunities expand, the benefits will accelerate. Robotics, drones, and artificial intelligence will have a growing risk management role in society.

These technologies are greatly enhancing the awareness and capabilities of human security officers and other personnel while helping mitigate market challenges.

The security industry has traditionally relied upon manual efforts to deliver expected outcomes, and the reliance on manual operations will continue. However, over the past several years, we have seen an evolution in terms of technologies that have the potential to transform security services and improve and augment the capabilities of human security officers. Such technologies include ground-based robotics and aerial drones as well as artificial intelligence (AI) and other features that guide them.

Different aspects of modern technology will have different impacts on the evolution of security services, but each of these technology areas is delivering new ways to increase situational awareness and manage risk. Furthermore, these technologies have not evolved, nor have they delivered improvements to security services, in a bubble.

Robotic security technology has progressed as improvements in artificial intelligence, vision systems, mobile technology, and sensing have enabled advanced capabilities to be built into the robots. Consider how drone-based technology has transformed as battery life has been extended, autonomous navigation has improved, and vision capabilities have vastly expanded. On top of the enhanced operational capabilities of such technologies, the requirements and capabilities around managing the data that such devices are producing are eliminating the boundaries between operational technology (OT) and information technology (IT), driving the need for collaboration between these two traditionally separate functions.

Like many industries and markets, the security industry is facing an inflection point as modern digital technology is delivering advanced and disruptive capabilities. However, simply deploying modern technology for the sake of having the latest and greatest is not enough. Technology decisions must be measured and strategic, and deployments must account for multiple tactical considerations. This paper is designed to provide an understanding of the implications of such technology for security practitioners and deliver guidance designed to support the procurement of "next-generation" (next-gen) security equipment.

Four Keys to Evolving the Security Technology Procurement Process

The tools of the modern enterprise have advanced significantly and rapidly, and this progress has led to the convergence of people, physical assets, and intelligent software. As robotics, drones, artificial intelligence, facial recognition, natural language interfacing, and other sensing capabilities come together across the security technology landscape, organizations are finding that they need to rethink their approaches to acquiring security-related services and technologies.

Indeed, the sophisticated and digital nature of such technologies is pushing the acquisition of next-gen security technology into the realm of digital transformation, which is something that is best accomplished through collaboration between lines of business (LOB), in this case security and IT. Digital transformation is a key reason for organizations to rethink and reshape their procurement practices of physical security.

The challenge, however, is that procurement relative to security devices has been different from the policies and procedures that have historically governed pure technology-related purchasing decisions. Security practitioners must take an active role in technology purchases and, at times, must lead these efforts when the technology is specific to security. The question now becomes, how does an organization rethink and redesign its approach to its security procurement processes?

To address this challenge, security practitioners should consider four key elements that are critical to delivering practitioner-led security technology procurement:

- **Identify the opportunity and spell out the value proposition.** Evaluate the current state of the security practice and identify deficiencies in existing processes. Identify and document how robots, drones, or any other next-gen security technologies will positively impact the overall operation. When taking on such an effort, be sure to zero in on the key metrics that are most important to the business. Keep in mind that it is not always about cost; the value proposition could be more about alignment of the security operation with the digital transformation efforts of the broader organization.
- **Know the strategy of the IT organization.** Modern security technology carries with it a significant IT-related element. For example, the use and management of connected assets such as security robots require a certain amount of software. Furthermore, these tools are essentially mobile data platforms; this data can be valuable to the organization, but the IT staff must be aware, engaged, and incentivized to support these investments. Get to know what is important to the IT organization, and use that insight to craft the appropriate opportunity statement. Further, create an alignment with the IT organization and work with the IT team to get this group's support.
- **Take ownership.** Yes, security robots and other next-gen security technologies are IT related. However, these tools are designed to enhance the capabilities of security practitioners. Security practitioners have a responsibility to be engaged and lead the effort to acquire the best possible tools for the job. Research the market; know what options exist, how others are deploying such technologies, and what benefits others have achieved. Use this information and take it to organizational leadership to highlight the value of next-gen security technologies.
- **Actively engage in breaking down operational silos.** Become a force for collaboration. Modern technology purchases are being driven by collaborative efforts between security and IT. Break the cycle of siloed procurement by actively engaging in strategic internal partnerships with IT to collaboratively define the role of next-gen security technology. Through such collaboration, the security function and IT function can reduce friction and increase operational alignment.

Security practitioners who follow these keys to driving the procurement process will find much higher success rates in terms of gaining budget approval to bring in modern security technology compared with those who do not.

Operational Environment Considerations

When organizations are deciding whether to leverage robots for security, they should consider the following factors about the operating environment that will contribute to the successful use, or lack thereof, of robotic security technology:

- **Indoors versus outdoors.** Will the robots be operating inside a building, outside in a parking lot, or on rough uneven outdoor surfaces? Other similar questions must be considered. Security robots are built to be mobile, but they are not built to traverse all kinds of surfaces. In addition to mobility, ruggedness also must be considered.
- **Flat surfaces versus uneven or sloped surfaces.** Robots are not all built with the same degree of mobile capabilities. When planning to deploy security robotics, organizations should consider the type of surface on which the robots will be working. This will help determine which vendor and which robots are best suited for the operating environment.
- **Connectivity.** How reliable is the Wi-Fi and network connectivity in the operating environment? Security robots are connected devices and should be able to communicate, in real time, back to the manned security station at all times. If connectivity is unreliable, this issue would need to be addressed as part of any initiative to deploy security robotics.
- **Population of the operating environment.** How many people and pieces of mobile equipment will be present in the operating environment? Although robots are built for safe mobile operations around humans and equipment, highly populous environments may affect their movement capabilities.
- **Specifics around sensing.** Security robots can be equipped with a wide range of sensors. Will the robots require specific sensing capabilities to effectively operate in the environment? For example, is there a reason to have radiation detection, smoke detection, CO2 detection, heat detection, humidity detection, and so forth? Organizations need to know what types of scenarios may exist within the operating environment and equip the robot with the appropriate sensing capabilities.

The previously referenced points represent a few key issues to consider when determining whether security robots are appropriate for the environment and which robot to select. This is not meant to be an exhaustive list - each environment has some unique features, but it does represent a good starting point from which to build out a security robot selection plan.

Similar operational environment considerations can be used when thinking about drones for security operations, including, but not limited to the following:

- **Fly zone versus no-fly zone.** Not all areas are approved for aerial drone usage. For example, sites near an airport are not authorized for the use of drones. Organizations need to know the legalities regarding drone usage around the operational environment.
- **Range of operations.** Drones are limited by battery life and therefore have a limit to the distance they can travel.
- **Rural versus urban.** There are legal issues around the use of drones in different places. Also, organizations that use this technology in population-dense areas with an abundance of man-made structures will face restrictions and challenges.

Again, this list is not meant to be complete; rather, it is a place to start.

Key Considerations When Evaluating Security Robotics and Engaging in Vendor Selection

Organizations should consider not only the operating environment but also the features, functionality, and capabilities of autonomous security technologies (robots and drones). When selecting a vendor for robots or drones for security operations, technology buyers should consider the factors in Tables 1 and 2.

TABLE 1: ***Security Robot Considerations***

Operational Considerations	Technical Considerations	Supplier Considerations
Movement capabilities (indoor flat surface versus uneven surface versus outdoor rough terrain)	Fixed sensor options or ability to customize sensor requirements (what sensors are available)	Financial stability
Bidirectional communication capabilities	Interactive touchscreen or not	Customer support structure (24 x 7 x 365)
Self-navigating or stationary	Audio capabilities	Degree of industry expertise
Real-time communication with manned security officers	Approach to navigation (restricted, simultaneous location and mapping [SLAM] based, vision based)	Robustness of partner/distribution channel
Remote operation capability	Reliability of connectivity	Single product or fleet of robots
Ruggedness of device (designed for indoor versus outdoor operations)	Sophistication of software interface	Product only or also providing services
Flexibility of the platform (ability to use across various use cases)	Sophistication of analytics capabilities	Sales model (as a service, lease, buy options)
Ability to interface with humans	Degree of AI, machine learning, and vision-based analytics on board	Remote monitoring and support options
Capability to support multiple environments	Power of onboard compute	Price
	Security (resistance to network security risks)	
	Size of the device itself (does it physically fit in the required environment)	

Source: IDC, 2019

TABLE 2: ***Security Drone Considerations***

Operational Considerations	Technical Considerations	Supplier Considerations
Battery life	Fixed sensor options or ability to customize sensor requirements (what sensors are available)	Financial stability
Charge time	Audio capabilities	Customer support structure (24 x 7 x 365)
Range of operation	Degree of autonomous navigation capabilities	Degree of industry expertise
Self-navigating capable or entirely human operated	Reliability of connectivity	Robustness of partner/distribution channel
Real-time communication with manned security officers	Sophistication of software interface	Single product or fleet of drones
Ruggedness of design	Sophistication of analytics capabilities	Product only or also providing services
Quality of video	Degree of AI, machine learning, and vision-based analytics	Remote monitoring and support options
Infrared, HD, night optics video capable	Power of onboard compute	Price
Nighttime and multidrone capable operations	Security (resistance to network security risks)	
Tethered or free-flying	Autonomous response capability	
Weight (>55lbs. requires FAA Part 107 compliance)	Security of data	
Payload capability		

Source: IDC, 2019

Tables 1 and 2 are meant to provide guidance relative to procuring robots or drones for the purpose of security. This is a new and evolving market, and the critical characteristics cited today may quickly become status quo as vendors in the space grow with the market.

Benefits of Deploying Next-Gen Technologies in Security Operations

Organizations that effectively deploy next-gen technology in their security operations to augment human security officers can expect several key benefits, including:

- **Enhanced effectiveness.** Modern technology is designed to deliver improvements to the business processes where the technology is deployed. In the case of robotics, drones, and AI in security, the technology is designed to deliver a greater ability to keep a facility secure. It can improve identification of a threat/risk, apply advanced analytics to support decision making and, in the case of drone technology, improve the ability to inspect a space and, if necessary, follow or track a threat. Providing human security officers with advanced capabilities allows them to leverage technology to help enhance decision making.
- **Augmented human performance.** There are certain things people can do, and certain things they cannot do, yet they can still achieve desired outcomes with the support of technology. For example, a human security officer can spot a person, but if that officer has not viewed a recent notification about the person, he or she may miss an opportunity to take action. However, a robot, a drone, or an AI-enabled camera would be able to run advanced facial recognition software to help a human officer realize that this person is someone of interest. This scenario played out recently in China when an elderly man went missing and the street cameras, equipped with advanced analytics and AI, were able to identify him, track him, and allow people to bring him home unharmed. This is just one example; the point is that next-gen technology is positively impacting the security industry by extending the capabilities of human security officers.
- **Mitigated labor challenges.** Studies have found that the annual turnover rate in the security guard industry is roughly 100% per year, with smaller security operations experiencing much higher turnover rates. Technology, such as robots and drones, is not meant to replace humans. However, with this technology, organizations are better equipped to identify security officers who are reliable while reducing reliance on those who are not. Additionally, across various industries, the deployment of modern technology has resulted in improvements in employee morale, helping improve employee retention. These workers will need to learn new skills to better operate in an environment with modern technology, but this is a positive in that it helps develop employee skill sets. Furthermore, the cost of labor is something to consider. While the intent is not to displace the workforce, there will be scenarios where there can be less reliance on the least effective workers. Technology is deployed to enhance the capabilities of the remaining workforce, it will translate to a lower cost of labor.
- **Aligned strategies.** As security relates to digital transformation, organizations must look holistically at their operation. The notion of digital transformation is to leverage modern digital technology to improve decision making. Indeed, the use of next-gen technology in security will address this point. Such technology can go beyond sense and respond. With digital technology, an organization is equipped to learn much more about overall operations than it would by relying on traditional manual efforts.

The preceding list of benefits is not exhaustive, but it highlights a few key advantages that organizations can expect with modern security technology. Those that have deployed the technology will likely note additional benefits that they have realized, but the four benefits identified above are key drivers of the adoption of next-gen technology in security.

Indeed, the benefits identified strongly relate to the four key elements in driving security practitioner–led procurement. Each of these elements should be considered when building out the business case for investment in next-gen security

technologies. Wherever possible, organizations should compare the benefits they achieve with security operations now to the benefits they could achieve with security operations in the future. This comparison will become the business case to drive investment.

Considerations

The benefits of using next-gen technology in security point to a technology that has tremendous disruptive potential to an entire industry. However, this technology cannot be deployed without giving due consideration to how it will impact operations. While the technology is designed to augment human performance and provide enhanced capabilities to human security officers, it will also drive reduced reliance on human security officers. This may be a good thing for an industry facing 100% turnover annually, but it's still something that bears considering. Indeed, the deployment of such technology will allow a human security officer to do much more than the officer could do without support from automation and AI. If turnover is not an issue, the focus then shifts to the benefit of significantly enhancing the abilities of security officers. Again, if this benefit can be quantified (such as reduction in response time), it will help generate approval for spending on the technology.

Another point worth considering is that this industry has relied upon video cameras for a long time; with cameras mounted in so many places, it's rare to be in a public area that does not have them. Over time, the technology has evolved, delivering high-definition cameras that can tie back into an AI-enabled monitoring station. Organizations will want to leverage the existing infrastructure and can do so by replacing outdated camera technology with more modern cameras.

However, cameras are largely fixed (pan-tilt-zoom [PTZ] capability does not change the fixed nature of cameras), and because of the ubiquitous nature of cameras, there is the possibility that they have become less effective as a deterrent and more relied upon after the fact. Security robots, by contrast, come equipped with cameras and deliver the ability to leverage autonomous mobility and thus provide physical presence that can act as a deterrent and can be easily redeployed. Past investments in camera technology can be a barrier to procurement. To break down this barrier, organizations should focus on the extended capabilities of the security robot — that is, that the technology goes beyond audio/video capabilities. They should present the case for robots as a deterrent and as mobile devices that can be equipped with a variety of sensors and communications capabilities that are not possible with fixed cameras.

Further, drone technology has its own hurdles to clear relative to where the drones can be deployed and used. While the use cases are certainly there for the use of drones in security, they have not yet become mainstream. The regulatory environment for drones, since they are aircraft, makes this a very challenging element to navigate. Battery life is also an issue to consider. However, using drones for limited patrolling and spotting, instead of continuous operation, will still deliver value from this technology. To gain approval for drone technology, organizations must identify the use cases and detail how the devices will improve the output of human security officers. Security practitioners who are showcasing the ability to extend sightlines and visibility while reducing risk to humans are gaining the opportunity to make this investment.

Anytime a new technology is developed, there is an adoption curve. Right now, we are on the early side of this curve relative to the use of robots, drones, AI, and next-gen technology in general. This is not limited to just security; it is the case across all industries and use cases. The technology, though, continues to progress, and as more organizations adopt it, the benefits will become increasingly apparent. Security practitioners can leverage the successes of those that have already made these investments to help them build their own business cases.

Conclusion

Modern technology is proliferating throughout business and society. As next-gen technology advances, the use case opportunities expand, and the benefits accelerate. Robotics, drones, and AI, in particular, will have a growing risk management role in society.

These technologies are greatly enhancing the awareness and capabilities of human security officers and other personnel while helping mitigate certain market challenges. From the perspective of both the provider and the user of security services, next-gen technologies should be a part of broader digital transformation strategies and efforts to bring together IT capabilities with OT functionalities.

Like all new developments, robotics, drones, and AI present unique challenges to users, forcing them to think about their operations — as well as their procurement processes — in new ways. With guidance, though, users can adjust to the evolving demands and reap the functional and financial rewards that can come with successfully implementing disruptive technologies.

MESSAGE FROM THE SPONSOR

About the Security Industry Association

The Security Industry Association (***www.securityindustry.org***) is the leading trade association for global security solution providers, with about 1,000 innovative member companies representing thousands of security leaders and experts who shape the future of the industry.

SIA protects and advances its members' interests by advocating for pro-industry policies and legislation at the federal and state levels; creating open industry standards that enable integration; advancing professionalism through education and training; opening global market opportunities; and collaborating with like-minded organizations. As the premier sponsor of the ISC expos and conferences, SIA ensures that its members have access to top-level buyers and influencers, as well as unparalleled learning and networking opportunities.

About the analyst:

John Santagate, Research Director, Service Robots

John Santagate is a Research Director at IDC responsible for the service robotics market. Mr. Santagate's core research coverage includes market trends and forecasts for service robotics, business process evolution through the use of service robots, and the integration of robotics into business processes and business IT architecture.

IDC Custom Solutions

IDC Corporate USA

5 Speen Street
Framingham, MA 01701, USA

T 508.872.8200

F 508.935.4015

Twitter @IDC

idc-insights-community.com

www.idc.com