An IDC White Paper, sponsored by Dell Technologies and Intel

IDC | ANALYZE THE FUTURE

PLANNING FOR A SAFER AND MORE SECURE FUTURE:

Leveraging New Data Types for Competitive Advantage and Revenue Generation

RESEARCH BY:

Mike Jude
Research Director, IDC

November 2020 | IDC Doc. #US46960420

Navigating this White Paper

Click on titles or page numbers to navigate to each section.

IDC Opinion

The safety and security market is experiencing a widespread transformation driven by an increasing need to integrate intelligence into video analytics and to leverage security telemetry to support many more business functions.

This rapidly evolving dynamic is forcing the industry to completely rethink how to homogeneously manage and analyze sensor data from the edge. Yet, even though the needs and technologies are rapidly changing, a recent study conducted by Dell Technologies, Intel, and IDC discloses a widespread confusion over the capabilities that will be required in the future or even how to assess the value of new solutions. Complicating this situation is the changing nature of security, where the very concept of security is expanding to include not only company assets and employees but also an organization's ability to leverage security data to conduct business and be innovative to remain competitive. Organizations that are not ready to adopt a new approach are likely giving up a significant competitive advantage: one that has the potential to drive down costs and enable a flexible response to changing security demands.

New approaches to safety and security are required. Similar to the way in which telephone companies have had to shift from purpose-built appliances to virtualized infrastructure in order to deliver on the promise of 5G connectivity, security operators must do the same and for largely similar reasons. The infrastructure needs to be able to adapt to rapidly evolving use cases and technology such as, in the security space, advanced analytics and ever-greater integration between, and automation of, disparate systems like access control, lighting, and HVAC.

While safety and security initiatives are increasingly vital to the protection of employees and company IP from nontraditional threats, they are also being leveraged to optimize company operations. This calls for a shift to a hyperconverged approach, which recognizes the need for multiple-use technologies. Yet uncertainty over the best way to do this has many IT, security, and business decision makers wonder what an optimal safety and security strategy and infrastructure would look like; in other words, what is the safety and security future state and how do we get there?

As this paper discloses, the future state is one where safety and security is driven by the collection and application of data for business processes. Achieving this future state will require a new approach to value assessment as well as a new way to think of such considerations as the degree and placement of computing and storage assets, the application of cloud services, and how physical security will be integrated with existing applications and cybersecurity. It will no longer be enough to think of safety and security as a standalone function but as an integrated part of a larger converged or hyperconverged computing and communication infrastructure.

The research conducted for this paper, which involved a global survey, cutting across industries such as healthcare, transportation, retail, and safe cities, of 705 IT and security professionals, supports this viewpoint, and while survey respondents represent a variety of readiness states, the majority are beginning to realize that safety and security solutions, while necessary, will need to be justified just as any other business investment: How will these critical capabilities contribute to business viability and profitability?

It will no longer be enough to think of safety and security as a standalone function but as an integrated part of a larger converged or hyperconverged computing and communication infrastructure.

Situation Overview

As the survey data confirms, organizations are aware of the need to enhance safety and security. In fact, most organizations of any size have at least some interest in improving their safety and security capabilities as well as maintaining or expanding existing budgets to improve their security posture (across all respondents, the average safety and security budget was in excess of $1.2 million). Yet, for most of the survey respondents, the investment is not efficient and is spread across many point solutions. As one interview subject from a large transportation company noted:

> [W]e are not as much integrated with our safety and security as you would have thought. We have some aspects that are and other aspects that are not …

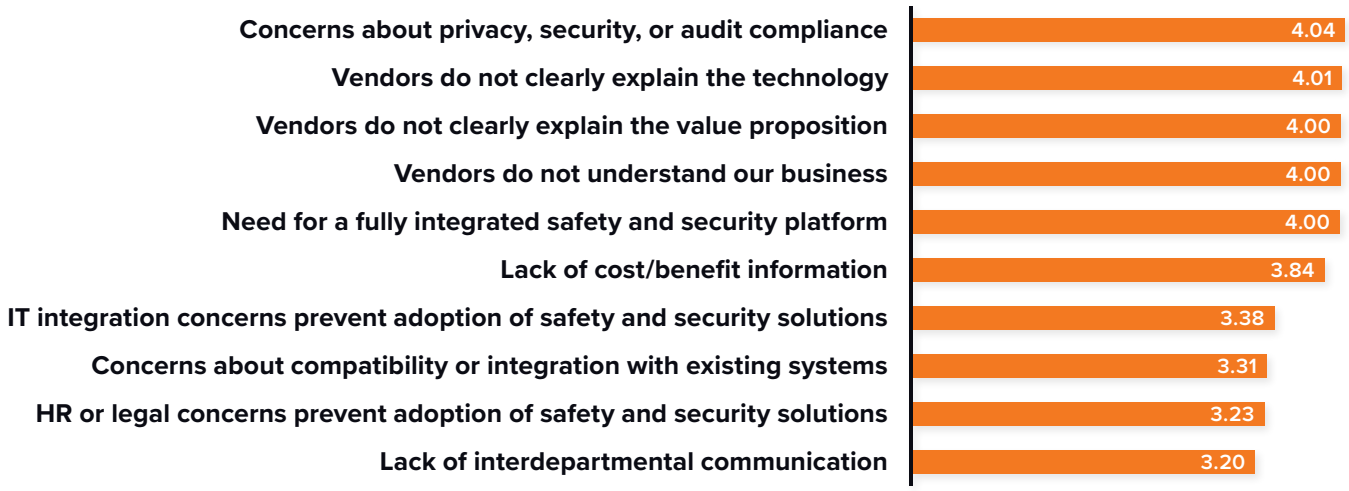
Furthermore, as IDC expected, results from the survey indicate that there is a rising interest in improving safety and security capabilities. In addition, there is a developing consensus that new approaches to safety and security will require the application of new technology. However, respondents are worried about potential barriers to the deployment of newer security solutions.

Although respondents believe that there is an increasing need for safety and security solutions (with more than 76% of respondents rating the need to protect the organization as either highly impactful or impactful), there are several major concerns that arise when planning for new capabilities. As Figure 1 illustrates, across all respondents, the need for privacy and auditability top the list of adoption concerns, followed by concerns that vendors of security solutions do not adequately explain the technology or value proposition of proposed solutions. This is followed by a concern that vendors do not understand the business of the organization and, finally, in the top 5, a concern that fully integrated solutions are needed.

FIGURE 1

Potential Barriers to Adoption of Safety and Security Solutions

(Scores based on a scale of 1–5, where 1 = no impact at all and 5 = high impact)



Source: IDC's *The Future of Safety and Security Global Survey,* August 2020 | n = 705

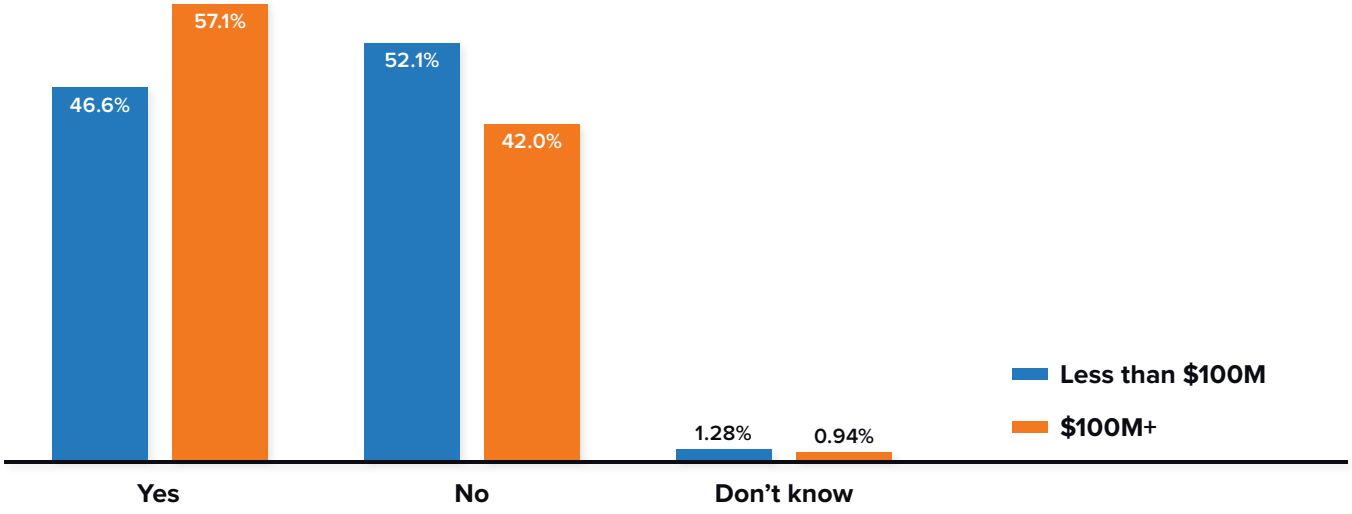
Although the survey results indicate some uncertainty associated with deploying new safety and security solutions, the results do indicate that the organizations, especially larger ones, are planning for a new future state. As shown in Figure 2, respondents from organizations with operating budgets over $100 million report that they are developing plans for future safety and security analytical improvements. Even nearly 50% of smaller companies report that they are planning as well.

FIGURE 2

Plans for Adding or Augmenting Future Safety and Security Analytics Capabilities

Q. Does your organization have a detailed plan for adding or augmenting safety and security analytics capabilities?

(% of respondents)



Source: IDC's *The Future of Safety and Security Global Survey,* August 2020 | n = 705

Nevertheless, as the survey also disclosed, budget constraints may limit the degree to which new solutions can be implemented. Nearly 50% of those surveyed indicated that their safety and security budgets would remain the same. Only a little over 39% thought their budgets would increase.

How is this conflict between increased awareness of the need to augment safety and security and the recognition that budgets will not likely increase be resolved? How can a new future state be architected that satisfies both?

Future Outlook

The answer is that safety and security can no longer be considered a standalone application that satisfies only one organizational need. In fact, safety and security technology—such as sensors and video cameras—can be employed in many valuable and interesting use cases. Increasingly, organizations are coming to understand that investments in technology can no longer be considered in isolation; survey data indicates that organizations are, in fact, thinking about future safety and security needs.

This all begins with a vision of what's included in the future state.

Envisioning the Future Market and Infrastructure

The future state of any technology-dependent market is fundamentally a question of the degree to which the technology is perceived as a necessary adjunct to organizational operations. In the case of safety and security, respondents agreed with the ideas of an enhanced need for safety and security technology. Survey respondents believe that ensuring the safety and security of organizational assets would become one of the most important considerations of doing business in the next three to five years. Sixty percent of respondents either strongly agreed or agreed and only 4% of respondents strongly disagreed.

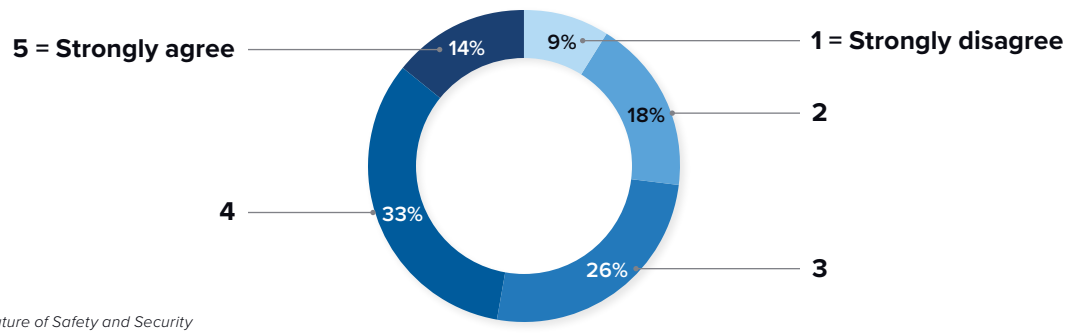
The survey data provides compelling support for the notion that the future state of safety and security is going to be highly dependent on advanced analytics. These analytics will utilize artificial intelligence (AI) and machine learning (ML) to provide many new capabilities, to both offload security personnel and provide new capabilities beyond the human operator. As shown in Figure 3, the survey data shows that AI is expected to become a large part of the use of video observation.

Survey respondents believe that ensuring the safety and security of organizational assets would become one of the most important considerations of doing business in the next three to five years.

FIGURE 3

Artificial Intelligence Will Increasingly Define Video Observation

(% of respondents; scores based on a scale of 1–5, where 1 = strongly disagree and 5 = strongly agree)



Source: IDC's *The Future of Safety and Security Global Survey,* August 2020 | n = 705

Cloud capabilities, too, will become important as advanced analytics demand more readily accessible storage and as applications become more complex, as noted by one of the interview subjects who manages the security infrastructure of a large healthcare network:

> *I think that over time, we're going to see a heavy expansion of cloud for just about everything that is currently done in on-prem datacenters across the industry, not just safety and security but just about everything. I think we're going to see that for flexibility, the capability of being more agile, as well as from the standpoint of cost.*

Of course, a shift to a more analytical approach to safety and security implies a new market approach to delivering such solutions. As noted previously, currently, organizations do not believe that solution vendors do a good job of explaining either their technology or value proposition. This implies a future state where the vendors and their delivery channels will need to both understand customers' businesses and their business processes so that solutions can be tailored to customer needs in a more holistic way.

Addressing the safety and security future state now:

According to Dell Technologies, the Dell Technologies and Intel teams worked with Genetec, a manufacturer of unified security, public safety and operations, and business intelligence solutions, to address safety and security needs across the globe. Dell Technologies and Intel supported with tightly integrating Dell Technologies workstation, server, and storage solutions with Genetec software to optimize its solutions prior to deployment. According to Dell Technologies, this enabled significantly faster data throughput and created factory-integrated, unified security solutions that significantly accelerated time to value for Genetec customers.

Building the Next-Generation Safety and Security Infrastructure

As the importance of safety and security increases the need for more capable solutions, the tension between budgets and needs will increase. This can only be resolved if safety and security solutions can be utilized as other technology investments—to assist in the generation of revenue or operational efficiency.

To date, safety and security infrastructure (e.g., video cameras) has been used to extend the reach and multiply the efforts of security personnel charged with observing secured spaces. However, video and other telemetric data can be even more useful when applied to optimize business processes. For example, video observation can identify high-use areas and traffic flow through a facility. This can be used to inform the use of HVAC and other facility resources so that energy can be used efficiently. It can also be useful in managing delivery of components to manufacturing lines or tracking inventory through a warehouse.

In fact, the key to extending the use of safety and security telemetry is tied to advanced analytics. These analytical applications can be large consumers of data storage, networking, and computational assets, requiring the involvement of IT and network management. The implications of such considerations lead to imagining a much different architecture for safety and security. While the current approach is appliance based, treating every new camera or sensor as another networked device with bandwidth and storage requirements, the future state needs to approach safety and security as a new source of business-specific data; data that can be leveraged for many purposes.

A future-state architecture utilizes the cloud but does not totally depend on it.

In a future architecture, analytics will take place at every level of the architecture. Edge devices will incorporate intelligence (i.e., analytics capabilities) that will drive new applications. Edge devices will perform analytical functions such as threat identification, but more comprehensive analysis, such as developing heatmaps of traffic patterns within a retail space, will be conducted in the core or even in the cloud. Storage too will be distributed, depending on the need of the application.

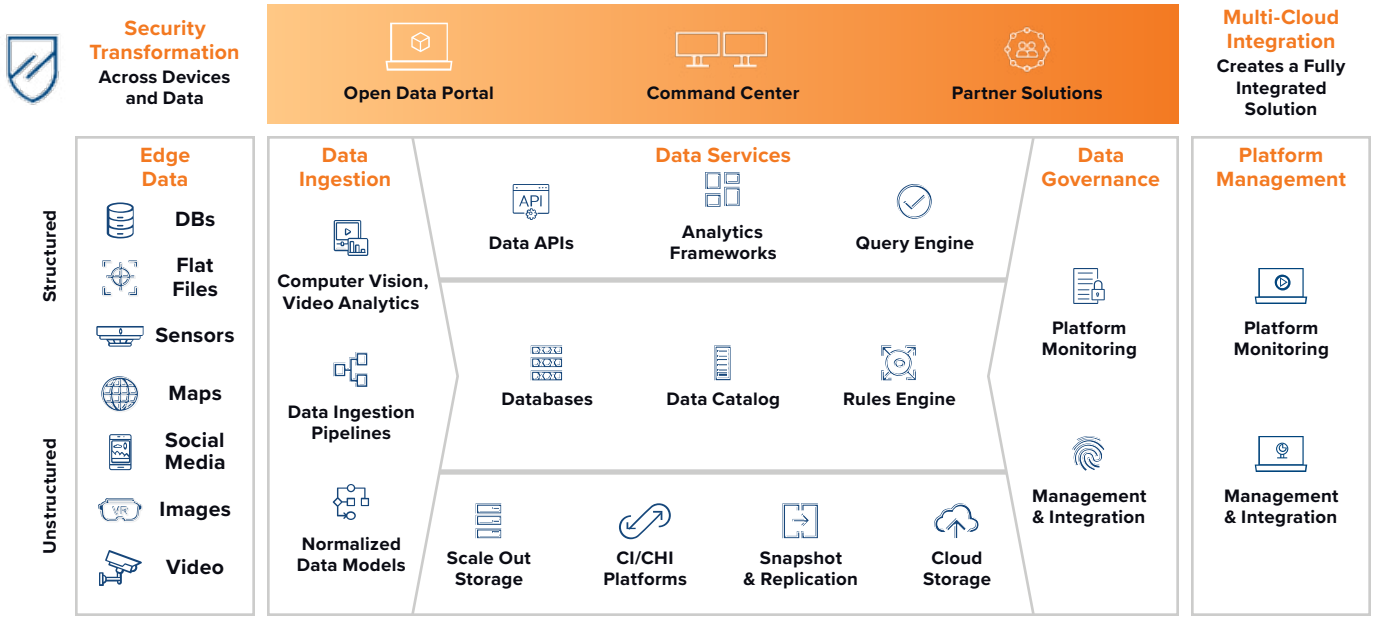
Also noteworthy is that a future-state architecture utilizes the cloud but does not totally depend on it. Cloud will be used for archival and heavy analytical functions for which large data sets are required, but much of the data load will be maintained at the edge, in devices and edge computing.

Integration, too, is important to a future state that can serve many applications. In terms of both integrating with existing infrastructure and applications and integrating across different technology verticals, respondents perceived a need for integrated solutions. In the case of video observation, nearly 60% of respondents strongly agreed or agreed.

Figure 4 illustrates a potential safety and security architecture that implements many of these concepts.

FIGURE 4

Example of Future Safety and Security Architecture



Source: Dell Technologies, 2020

Taking a complete solution view: one where considerations such as supporting an Internet of Things (IoT) is an important requirement but so is acknowledging that core storage, back-end server computing, and robust networks will all be needed. In other words, any safety and security solution in the future must be assessed from a holistic point of a view rather than a point solution perspective.

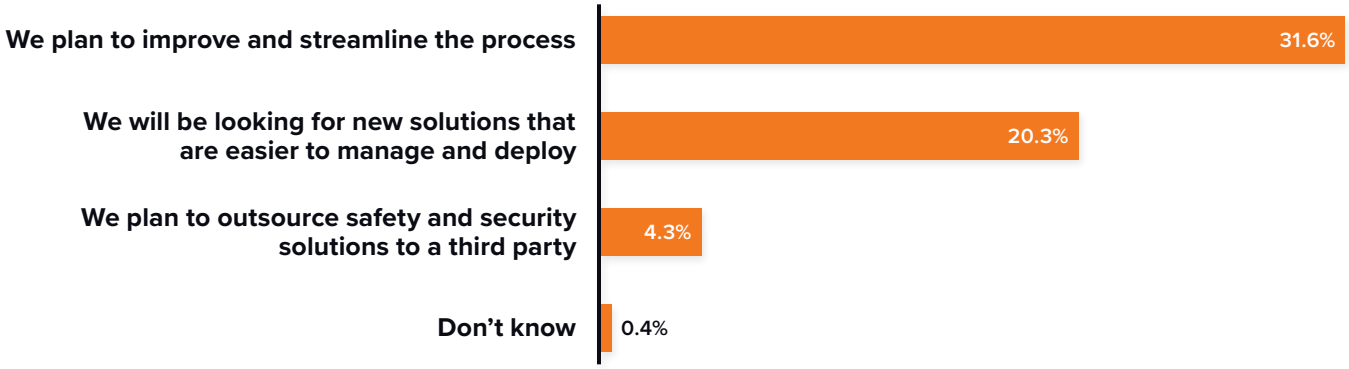
Of course, simply implementing what could be a very complex infrastructure is not an appealing vision. Survey respondents felt that improvements in the delivery of safety and security solutions would be necessary. As shown in Figure 5, improvements in delivery and the desire for solutions that are easier to deploy top the list.

FIGURE 5

The Majority of Organizations Anticipate Change in the Way the Organization Delivers Safety and Security Solutions in the Future

Q. Do you anticipate the way your organization delivers safety and security solutions to change in the future?

(% of respondents)



Source: IDC's *The Future of Safety and Security Global Survey,* August 2020 | n = 705

Ease of use is generally tightly coupled with cost to implement because the easier a solution is to install, the less time it takes to do so. This translates into lower labor and training costs and is an important consideration when evaluating potential safety and security solutions. Historically, the cost of a safety and security solution was simply the premium paid to ensure security. As the primary consideration increasingly becomes one of assessing value, the focus is shifting to evaluating both the cost and the benefit of implementing technology. Not only should the cost be minimized, but the benefit should also be quantifiable. Value is evaluated in terms of the degree to which a technology supports revenue-generating activities. For example, in the case of retail, video observation combined with analytics can be used to inventory shrinkage, and the value can be assessed in terms of the degree to which losses are reduced.

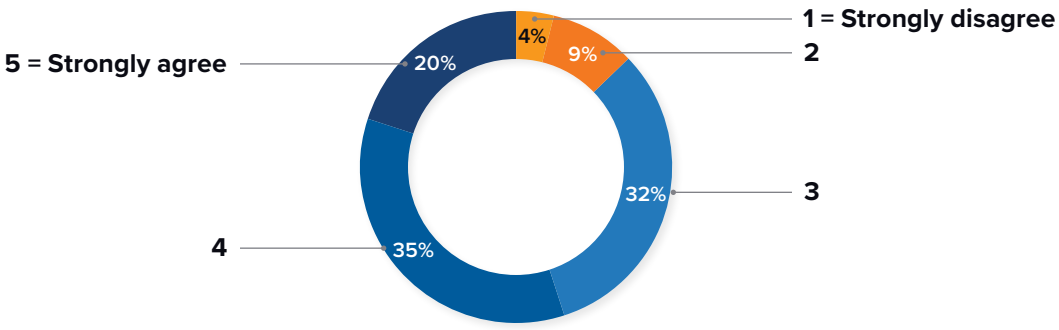
Not every cost or benefit is definable in terms of organization activities though. Risk can come from outside of organizational control, and as a result, the future state will also be defined by externalities to the market. How will regulation, for example, impact the deployment of safety and security solutions? The respondents to the survey felt that regulation as well as the need for internal regulatory compliance activities such as audits would be a major concern (see Figure 6).

FIGURE 6

About 87% of Organizations Agree That in the Future Regulators Will Become Increasingly Concerned About the Privacy Violation Implications of Video Observation

Q. Please indicate the degree to which you agree with the following assertions on the future (next three to five years) of safety and security solutions: Regulators will become increasingly concerned about the privacy violation implications of video observation.

(% of respondents; scores based on a scale of 1–5, where 1 = strongly disagree and 5 = strongly agree)



Source: IDC's *The Future of Safety and Security Global Survey,* August 2020 | n = 705

Aligned with the concern for regulatory oversight is the concern for organizational pushback. Survey respondents felt that employee resistance to new safety and security capabilities could also be an impediment to adopting such technology in the future. Nearly half of those surveyed (43%) expected such resistance.

In addition, simply changing technologies does not guarantee a return on investment. The way in which a technology is deployed and supported can also have a profound impact on the value that is realized, and this depends on the ability of the workforce to implement the future state.

Workforce Transformation

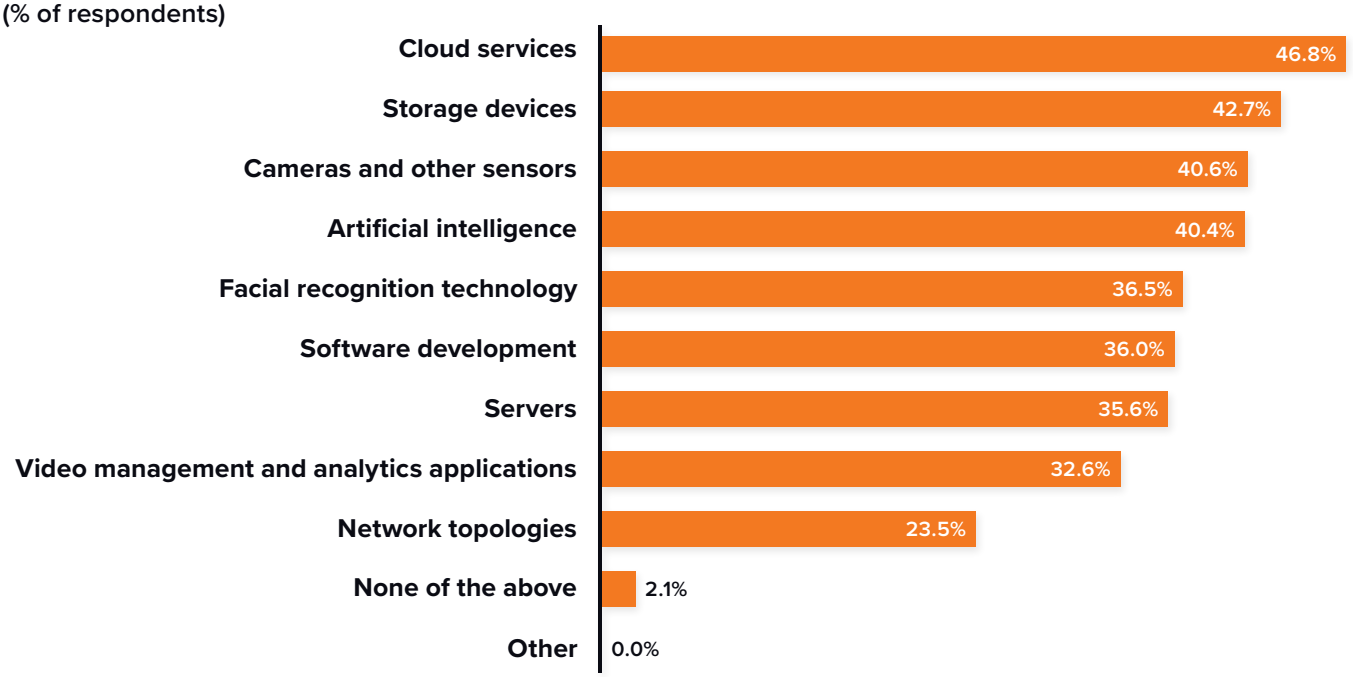
A new approach to safety and security requires an organization that understands how to not only implement it but also apply the capabilities it provides to other business needs. This will likely combine the expertise of facilities management with an IT appreciation of advanced analytics. Survey respondents believed that new skills would be required to implement the future state. As shown in Figure 7, respondents felt that the top 5 core competencies required in the future would be a knowledge of cloud services, storage devices, cameras and other sensors, AI, and facial recognition technologies.

FIGURE 7

Core Competencies Organizations Need to Acquire to Implement Safety and Security Solutions in the Future

Q. What core competencies do you think your organization will need to acquire to implement safety and security solutions in the future (next three to five years)?

(% of respondents)



Source: IDC's *The Future of Safety and Security Global Survey,* August 2020 | n = 705

While some of these skills are undoubtedly already inherent in IT organizations, most are new notions to the facility management organizations. This implies that some significant organizational change is required to address this future state. Survey respondents also indicated that there would be a closer working relationship between IT and physical security. More than 50% of respondents thought that there would be a closer relationship, while only 6% of respondents strongly disagreed.

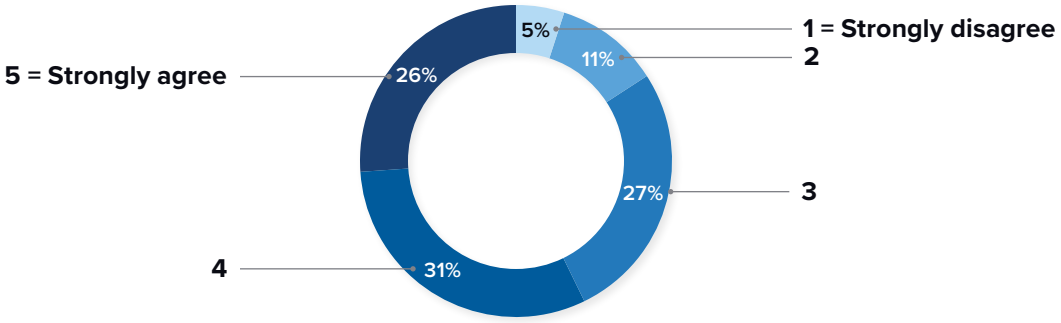
This merging of organizations along with the adoption of application-centric technology by the physical security organizations also portends a more holistic view of security: one that integrates physical and cybersecurity applications to enable new capabilities — for example, enabling application access based on the proximity of an employee to an authorized terminal device. As shown in Figure 8, 57% of those surveyed indicated that physical and cybersecurity would merge and only 5% strongly disagreed.

FIGURE 8

Most Organizations Agree That the Next Wave of Enterprise Security Will Be the Integration of Physical and Logical Security

Q. Please indicate your own level of agreement with the following statements: The next wave of enterprise security will be the integration of physical and logical security.

(% of respondents; scores based on a scale of 1–5, where 1 = strongly disagree and 5 = strongly agree)



Source: IDC's *The Future of Safety and Security Global Survey,* August 2020 | n = 705

These considerations lead to the following conclusions about the safety and security future state:

- Safety and security will become an **integral part of doing business** and a **competitive advantage.**
- The next generation of safety and security infrastructure will be **technology centric.**
- **Advanced analytics** will define safety and security solutions.
- Safety and security solutions will drive an **increased demand for storage and other networked assets.**
- Safety and security **budgets will not likely increase substantially** as a percentage of overall operating costs.
- **New skills and organizations will be required** to implement the future state.

Challenges/Opportunities

This brings us to the question of how we get from where we are to this future state? While the notion of rearchitecting the safety and security infrastructure may seem to introduce some significant challenges, it also presents the organization with some significant opportunities as well.

Challenges can be summarized as: the need for a comprehensive plan for safety and security, the need for organizational changes, and budgeting.

Planning

In the case of planning, the key is developing a plan that is tightly integrated with planning for other IT-centric capabilities. However, it is critical that such planning be done with a complete understanding of not only what capabilities are required now but those that may be needed in the future. Such planning, therefore, requires the participation of not only IT and operational technology (OT) management but also physical security, facilities management and, in some case, finance. Such plans should also be reviewed with trusted vendor partners—those that have proven that they understand the organization's needs and business processes.

The key is developing a plan that is tightly integrated with planning for other IT-centric capabilities.

Implementation

Ultimately, a plan is only as good as the potential for implementing it successfully. The second major challenge is implementing an organizational structure that supports a new approach to safety and security. Plans must ultimately be implemented and maintained by the organization's workforce. Identification of skill deficiencies and an assessment of the organizational structure that will be charged with managing the future state are essential. Training is critical to address such deficiencies, so budgeting must include the cost of any training programs.

Budgeting

Budgeting is the third major challenge. It goes without saying that achieving the future state must be accomplished within the constraints of organizational budgets. While this would seem to be a zero-sum game when safety and security is considered in isolation, where such technology is implemented as an adjunct to a larger hyperconverged infrastructure, it is clear that cost cannot be the only consideration: benefit, the ability to increase revenue or organizational efficiency, becomes a major consideration. Solutions must be justified, not only on their ability to improve safety and security but also the viability of the organization from a financial perspective. In fact, if the survival of the company is the primary consideration, financial security must be included in the safety and security continuum.

Of course, there are significant opportunities as well.

Business Investment

Chief among those are the opportunity to leverage safety and security as a business investment and the opportunity to partner with trusted vendors to leverage their expertise to implement scalable, reliable solutions.

By considering safety and security as a source of business telemetry—one that can provide deep insights leading to process improvement—it is possible to treat safety and security as any other business investment: one that has a cost but also a return.

Value Opportunity

Probably, the most important opportunity is that of approaching safety and security as a value opportunity rather than an insurance policy, which provides a way to transcend budget and organizational problems. By considering safety and security as a source of business telemetry—one that can provide deep insights leading to process improvement—it is possible to treat safety and security as any other business investment: one that has a cost but also a return.

An additional opportunity is to partner with vendors to ensure that the needs of the organization are addressed while implementing a plan that will evolve as those needs change. Safety and security technology has traditionally been delivered to the market in the form of point solutions. Yet point solutions are no longer an option when every investment must contribute to organizational success. Partnering with trusted vendors to deliver more comprehensive solutions ensures that solutions will be more holistic. Not incidentally, such partnerships make vendor success contingent on organizational success.

Conclusion

As the research indicates, the future of safety and security is highly dependent on demonstrating business value in addition to that of simply securing the enterprise. Safety and security will increasingly be a set of capabilities whose underlying technology can be brought to bear to accomplish many things, some of which will contribute to the profitability and effectiveness of the organization.

Technologies such as video cameras and other sensors will be employed to reduce the friction of business processes, improving industries such as manufacturing and retail by tracking the flow of materials and products as well as the way in which workers and consumers interact with them. Safety and security analytical applications will also be employed to manage workforces by reducing the overhead associated with activities such as time reporting and tracking.

The bottom line is that as budgets continue to decline in comparison to the need, a converged approach to safety and security will increasingly be required. Technology to support physical security will increasingly need to be justified in terms of the value it provides rather than in terms of the insurance it provides. This new orientation will also require a new organizational approach within companies, one that combines the talents of facilities management, IT, and economic analysis. Such an organization will also need to have a deep understanding of the organizational value chain and be able to assess the impact of safety and security telemetry on process improvement activities. Some organizations are beginning to understand this new approach, but many are not. IDC believes that approaching safety and security as a competitive advantage rather than as a required overhead will be crucial to business viability: those that do not will be in a significant disadvantage in the market.

Technology to support physical security will increasingly need to be justified in terms of the value it provides rather than in terms of the insurance it provides.

About the Analyst

Mike Jude
Research Director, IDC

Mike Jude is the Research Director for the IDC Video Surveillance practice within the Cybersecurity Products Group. Dr. Jude's core research coverage includes video market dynamics and metrics, the application of video surveillance systems within a broader security framework, and video data analysis. Drawing on his background in telecommunications regulation, data network infrastructure design, video device technology, and space imaging systems, Dr. Jude's research also focuses on the regulatory and public policy implications of widespread video surveillance.

More about Mike Jude

Message from the Sponsors

Dell Technologies helps organizations and individuals build their digital future and transform how they work, live and play. The company provides customers with the industry's broadest and most innovative technology and services portfolio for the data era.

Learn more about Dell Technologies

Intel creates world-changing technology that enriches the lives of every person on earth. We are inspired to Drive innovation that makes the world safer, builds healthy and vibrant communities, and increases productivity. We will Harness our reach around the globe to better society, business, and the planet and push ourselves and our industry peers to be more responsible, inclusive, and sustainable. Intel will continue to engineer solutions for our customers' greatest challenges with reliable, cloud to edge computing, inspired by Moore's Law. We have big ambitions, and a growing sense of urgency to work with others and address world challenges no one can tackle alone.

Learn more about Intel

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

IDC Research, Inc.
5 Speen Street
Framingham, MA 01701
USA
508.872.8200

idc.com @idc

IDC Doc. #US46960420