

December 2, 2019

Ed Finkel, Contributing Writer

page 2

Contracted vs. In-House Guarding: No Universal Right Answer

continued

Cybersecurity presents a new set of questions in terms of what to outsource vs. keep in house, Oringer says. “The convergence of physical and cybersecurity threats – for example, an employee carrying intellectual property on a laptop to an annual meeting – presents new opportunities and challenges for CSOs and their IT counterparts in terms of monitoring, protection and control technologies and resources, as well as outsourcing decisions,” he says.

Chris Dunn, CEO of Covered 6, which provides an intensive five-week training program for security officers (see sidebar), says most entities he works with that have included Space X, Virgin Orbit and Pepperdine University, end up with a hybrid guarding model. “They need a better-trained person,” he says. “They’re dealing with active shooter, technology integration and other complex issues.”

Outsourcing means less liability and greater flexibility, Dunn says, but clients of his often prefer to have more control over training. In-house guarding units bring quality control and a greater ability to build teams and invest in enterprise culture, he says. But outsourcing provides backup for events and unforeseen circumstances. “The hybrid model is definitely better,” Dunn says.

Threats and Solutions for 2020

Enterprises face an ever-shifting array of threats and solutions in both the physical and cybersecurity realms. Oringer sees cybersecurity’s impact on physical security, the emergence of artificial intelligence (AI), the growth of the cannabis industry and outsourcing of security among municipalities to bolster their police forces as among the “megatrends.”

“Twenty years ago, nearly everyone worked under the same roof. Now, you have workers all over the place, connecting to your system. There’s more exposure,” he says. “Cloud computing and the Internet of Things has had a profound impact on the day-to-day operations of business and government, and presents interesting new security challenges to client organizations.”

AI has been important in taking a proactive approach to security, instead of observe and report, enterprises can collect, analyze and take action based on data, Oringer says. “We’re predicting when things could happen and potentially prevent things from happening,” he says, adding that’s an area where contracted enterprises can help. “Some in-house security operations might not have the resources to spend big time on AI.”

Collaboration between physical and cybersecurity has resulted partly due to adversaries’ growing ability to remotely threaten and attack anytime and anywhere, Oringer says, adding that active shooter and workplace violence remain significant physical threats. He sees an opportunity for guarding enterprises to strengthen their roles as trusted advisers by offering a mix of security consulting, innovative software and system integration capabilities.

December 2, 2019

Ed Finkel, Contributing Writer

page 3

Contracted vs. In-House Guarding: No Universal Right Answer

continued

When it comes to protecting information, Boeing has an internal Information Protection Board in place that helps guide the enterprise's long-term strategy, Komendat says. "We spend a lot of time, energy and investment to stay abreast of the current threat environment and implement the best solutions we can, to deal with adversaries that come after our information," he says. "There is a constant drumbeat of investment and collaboration."

Boeing remains well aware that it not only needs to develop new technology but it also needs to protect its proprietary information to maintain a competitive advantage, Komendat says. "The U.S. government does a good job of identifying nation-states that aggressively come after technologies – and Boeing and other enterprises pay close attention to those warnings," he says. "But you also have to be concerned about those within your network who are authorized to have access, and make sure you've got the right tools in place to make sure no one is taking information and using it inappropriately."

As the second-largest defense contractor in the U.S. and the largest aerospace enterprise in the world, Boeing's Information Technology & Data Analytics organization and Komendat's Security and Fire Protection team work together closely safeguarding the company's information and networks. "We collaborate very closely," he says, even though "the organizations are in different, functional verticals. But there's a common understanding. The things we develop, the technologies we work on, are really differentiators as we go out and compete in the world. Protecting that information is paramount."

Komendat adds, "Collectively, our job is to support each other and make sure that whether it's U.S. government information, or Boeing proprietary information, that it's protected appropriately and at the highest levels. Obviously on both the unclassified and classified networks, the threat environment is dynamic, and our responses need to be [dynamic], as well."

As an enterprise that has employees across the globe, Boeing faces a variety of physical security challenges, and needs capabilities to not only deter bad actors but also ensure the safety of those working in its facilities, Komendat says.

"Unfortunately, there are many unexpected situations that take place with regularity across the world, and we can't be naïve and think that similar situations couldn't impact us," he says. "We have to be prepared and keep events from impacting our people and assets as much as possible."

In addition to the traditional security methods, Boeing has been exploring the use of robots, drones, smart camera systems, new badging kiosks and technologies to improve security in the workplace. Komendat says that over the past couple of years, Boeing has found that while camera technology has matured greatly, some of the others are not quite ready for prime time at the scale necessary. "We are exploring some new ideas," he says. "We need reliable technologies that will improve security in the workplace and be more efficient."

December 2, 2019

Ed Finkel, Contributing Writer

page 4

Contracted vs. In-House Guarding: No Universal Right Answer

continued

Drexel University faces a variety of safety concerns associated with its location in an urban environment, Behr says. “We’re always looking to prevent people from going in and stealing unattended property,” she says. “We’re concerned about controlling access to buildings at night, and we’re always concerned about the safety of our students.”

Drexel responds to potential threats by keeping response plans up-to-date, conducting trainings with local law enforcement partners and upgrading equipment and technology, Behr says. As a university, Drexel doesn’t want all buildings locked during the day, so it has a mix of electronic locks, other access controls, cameras and patrols.

“We’ve added cameras, so we now have up to 640-plus inside and outside buildings, but we can’t monitor every camera 24 hours,” she says. “We’ve upgraded cameras over the past year and a half so we can be integrated with our partners in the city of Philadelphia. We are also changing our radio system to be compatible with city police.”

Drexel also cross-trains with city police, FBI and other law enforcement agencies, and hosted a tabletop exercise in May, Behr says. The university does constant public education, necessary in part because one-quarter of the undergraduate student population changes every year.

“We have partnered with our HR department to add public safety information into orientation for all new employees,” she says. “We’re working with the communications office to get information out. And our police department’s community

relations team has two officers who constantly engage with student organizations, Greek life and other departments.”

M&A Predictions for 2020

The past year brought an ever-increasing flow of mergers and acquisitions in the security space, which Keith Oringer, founder and president of Security ProAdvisors, sometimes helps broker and generally keeps tabs on across the industry.

For 2019, he sees Allied Universal’s acquisition of five companies as perhaps the biggest story. Allied purchased three guarding companies – Point 2 Point, Cypress and Shetler Security – as well as two system integrators, including Securadyne and Michigan-based Midstate Security.

Other major deals on Oringer’s radar have included Garda World’s purchase of Whelan Security, Securitas buying both Global Elite Group and MSM Security, and Prosegur cutting a deal with Telefonica for the latter to acquire 50 percent of its alarm business in Spain. And on the technology side, Vector Security bought ADS, and ADT purchased Life Shield, Oringer notes.

Oringer expects continued heavy activity in 2020, especially among the largest enterprises. “I don’t think anything’s going to change,” he says. “If we were to have a significant drop in the stock market and the economy, you would see valuations dip. We’re also going to continue to see merging of technology, what we call integrated guarding, with the on-site and mobile security officers and remote video monitoring.”