The Uberization of Security’s Business Model

Is it time to reduce the total cost of ownership for the security program?

- By Ed Bacco
- Mar 01, 2019

The increase in the direct costs to deploy and maintain physical and logical security systems such as access control, video management, communications, cyber defensibility and visitor control combined with the increase in the indirect costs needed to operate and support these systems, has reached a tipping point. Companies large and small are now actively seeking a fresh approach to optimizing their physical and logical security operations and managing their risk, while capping or reducing their total cost of ownership (TCO).

What we are now witnessing in the physical security space is very reminiscent of what we saw in the early years of the IT industry where many companies first deployed IT systems and computers and then because of the steadily increasing costs, started looking for a more economical way to support the deployment, maintenance and operation of those systems. The company that recognized the opportunity presented by the desire for companies to control their IT costs was Electronic Data Systems (EDS), which owned the lion share of the market for a very long time and led to the creation of the category of services commonly referred to as “outsourcing.”

By 1980, the outsourcing model was being used in other industries. For example, a Design, Build, Own, Operate, Maintain (DBOOM) contracting model was being used by energy services companies (ESCO) to provide measurable savings and advantages to government and business clients at every stage of their energy efficiency projects. Specifically, the value proposition for using this contract model is described by the following operational elements:

- Design: Drawing only from best-in-class energy infrastructure components without supplier bias, ESCOs can tailor a solution to maximize efficiency or to manage development costs.
- Build: ESCOs can partner with local contractors to complete a project or recruit internationally renowned experts to oversee construction, retrofitting or installation.
- Own: Clients can take control of the new facility or let the ESCO run it and manage energy delivery.
- Operate and Maintain (O&M): ESCOs can train existing staff to run on-site systems, take on all O&M responsibilities or recruit new staff to operate and maintain energy infrastructure.

The companies that deployed this model differentiated themselves from vendors that pushed specific solutions, limited contractor choices or required long-term contracts. The DBOOM enabled ESCO provided vendor independence and complete freedom of choice as well as measurable costs.

Slow to Adopt

So far, when it comes to systems and their components, the physical security industry has been slow to adopt the outsourcing model even though they led the creation of one of the largest “outsourced” markets in the United States, the $64+ billion uniformed guard services. The primary cause of this slow adoption rate is the lack of vendors who have the resources needed to support an outsourcing model. Additionally, the security market has a culture of risk aversion that is compounding the slow adoption rate.

Finally, the need to control the costs within the physical security space has been accentuated by the risk from cyber-attacks. The industry has become increasingly aware of the vulnerabilities that the physical security devices/systems pose to the security of the corporate networks. Chief Security Officers (CSO) are finding themselves stuck in between knowing they need the physical security systems and the awareness that those same systems may lead to a serious security breach. We call this the “Insecurity of Security.”

Faster, Better, Cheaper

The convergence of CSOs and CISOs wanting to reduce the direct costs and the indirect costs while mitigating the vulnerabilities of their systems is a watershed moment within the security industry that taken together will outweigh the individual concerns that prevented them from outsourcing the deployment, maintenance and operation of their security systems.

The scorecard for delivering a fully hosted suite of consulting, technology, and professional services, or IaaS, will include the ability to create a collaborative ecosystem of platform providers, application software vendors, and hardware vendors. Initially, the technology services will include access control, video management, visitor management and critical communications. However, “infrastructure” refers to some or all of the security technology infrastructure as well as the management, maintenance, metrics and reporting needed to fully leverage the investment. This can only be delivered by a SOC and NOC provider with a depth of integration and managed services pedigree as well as the consulting services to create and manage the program from the perspective of the CSO.

The underlining business model of IaaS is not a new one. Uber, VRBO, Airbnb, Wag and many others have been successfully leveraging a model commonly referred to as a “sharing economy.” The concept of a sharing economy has been morphing since it first appeared in the U.S. around 2014 and still today, no one can agree on a definition. At its core, the concept takes advantage of a trend where consumers don’t want to “own” something like a car, vacation home, bicycle or an electric scooter, and would rather just purchase the service in the exact amount they need and forgo the costs of maintaining them while those same things remain idle in the garage or in another city. On a very fundamental level, this represents a risk management strategy. On an individual level, the consumer can mitigate their financial risks by only consuming what they need.

The IaaS model is designed to take advantage of this emerging business model, by offering customers options to outsource the ownership and/or operation of their physical and our logical security systems. As previously mentioned, CSOs know firsthand how much it costs to install a physical security system. They are now becoming aware of the indirect costs to operate and maintain those systems, including the costs of servers, networks, switches, IT staff and system administration. At first glance, the indirect costs can range between 20 percent and 70 percent of the direct costs. More work needs to be done to fully validate these numbers, but it is safe to say, that indirect costs are increasing at a time that most corporate IT departments are looking to decrease costs through some sort of outsourcing model.

In addition to the direct and indirect costs of security, the attention of both CSO's and the Chief Information Security Officer's (CISO) are the vulnerabilities that are created by deploying physical security devices on the corporate network. Traditionally, these devices were either not designed with cyber hardening in mind, or if they were, they weren't being maintained with the same rigor of a laptop or desktop computer. In either case, the layer of security that was deployed to protect company assets may in fact, enable a breach. These vulnerabilities can be addressed at the device level, but again, most IT teams are primarily focused on protecting the most importance assets against an unceasing barrage of cyber-attacks. They have little patience, time or resources to spend on physical security systems. If a sharing economy model existed within the physical security industry, it would enable an enterprise consumer to purchase the services they needed without having to build, operate and maintain it. It would provide many more features that would be available at the time of need but today almost always go unused. The term "uberization" comes to mind. Uber recognized a demand for a car service that didn't require a person to buy, rent or wait for transportation through a dispatch system. They brought people together who had a car that wasn't being fully leveraged from a financial perspective, with the people who were willing to pay for a ride.

What Uber did for the car sharing service industry, IaaS could do for the physical security industry because it will, for the first time, provide corporate consumers options to purchase the physical security services they need, without having to buy the whole car.

IaaS will also raise the bar on the cyber security protection of the physical security devices through the direct monitoring of the devices through a 24/7 Network Operations Center (NOC) and/or the ability to air gap the network that the physical security systems ride on from the corporate network.

IaaS will also unlock other market opportunities by offering enterprise quality products and services to mid-market companies that traditionally lacked the financial resources needed to deploy a system of their own.