The McLean Group

CASE STUDY

Digital Transformation and Physical Security: A Call to Action

The physical security industry is extremely active right now, with an addressable market estimated at $124.9 billion for 2020 and growing to $232.5 billion by 2027. This growth reflects the increasing demand for security as traditional threats like terrorism and crime grow exponentially in terms of variety and technical sophistication. This trend is of course exacerbated by the global pandemic. However, as important as growth is that digital transformation and advancements in areas such as automation, artificial intelligence, cloud computing, and blockchain are all fundamentally transforming the sector and the way security companies do business.

Digital transformation involves the integration of digital technology from all areas of the enterprise into the security infrastructure. While digital transformation is exceptionally promising for the physical security industry today, the fact is not everyone will survive the journey. Significant portions of the industry are seriously lagging behind their more data-driven contemporaries. These companies risk becoming displaced and disrupting the entire security ecosystem.

The physical security industry was built upon precursors of digital transformation, which bodes well for a promising future.

About The McLean Group

The McLean Group provides mergers and acquisitions advisory services, business valuations, and growth capital to selected clients. Our investment banking and valuation practices are built on comprehensive industry knowledge, extensive transaction experience, senior-level attention to every client engagement and a real-time understanding of industry-specific value drivers. By partnering with clients and providing strategic advice through every phase of a company's development, The McLean Group is uniquely positioned to support our clients' long-term success. Learn more at www.mcleanllc.com.

Ironically, the security industry has been transformative for quite some time, stemming from early advancements in technologies that fundamentally changed its business long ago. IP-based cameras, for instance, were an early advent of the IOT sensor. Access control programs of yesterday constructed some of the world's first physical-digital identities. Security central stations had for years monitored customers' assets remotely and on a 24/7 basis. However, despite these advancements, the industry historically has not leveraged the gold mine of untapped data because it failed to think creatively, and instead opted to use products and data only for the purposes for which they were originally designed and failing to apply these solutions in unique ways to address more complex problems. A great example from the past would be only using CCTV cameras to solve a crime, but not using them for parking enforcement at the airport, as is so common today. The security industry years ago also rarely had the tools or skills in place to solve more diverse security problems, like using access control logs to proactively discover insider threats. To some degree, this failure had to do with architecture and purpose-built solutions as well as limitations of technology at the time.

Historically security professionals as well as end users were accustomed to a very regimented and siloed fashion of security information consumption. Over time, however, digital transformation opened up new opportunities for security practitioners to consume disparate data and solve new, outside-the-box security challenges. A great example today would be using cameras and video analytics to ensure ride safety compliance on theme park roller coasters, a capability largely due to advances in machine learning capabilities in these systems. Digital transformation also dramatically changed consumer demands, with an old-fashioned, manual, and relationship-based industry now expected to become data-driven, connected, always available, frictionless, and multi-purposed. Big tech end-users and smart entrepreneurs certainly met these expectations head on, but the rest of the industry has remained relatively stagnant. In fact, a 2018 Accenture-Microsoft Security Survey found little urgency in becoming more technologically savvy when it identified that only 30 percent of security leaders polled felt digital transformation was critical.

The big challenge is that the fate of the industry depends on far more than just "survival of the fittest". The security industry relies on relative strength across its interconnected economic ecosystem of end-users, manufacturers, integrators, consultants, industry organizations, and even investors and insurers. The industry's future hinges on a strong support structure and relative homeostasis across this ecosystem. Transformative end-users, for instance, rely on equally enlightened consultants to help scale problem solving, while transformative vendors need alignment from integrators to scale sales of products. Another reason digital transformation must be embraced throughout the security industry is that industry progress is reliant on the collective ability to consume disparate data from all kinds of sources and vendors. At its core, digital transformation is inherently about democratizing data, sensors, and infrastructure. Unfortunately, the added challenge here is that physical security still largely operates within large, closed-architecture systems that hold consumption hostage to vendor advancements.

For example, it doesn't matter how many transformative products a security systems integrator can sell if their project-based delivery model does not allow the customer to leverage the full capability of the products. Additionally, it doesn't matter if consultants take over as custodians of a growing subscription-based "security-as-a-service" model, if they insist on remaining vendor agnostic subject matter generalists. It also doesn't matter how many transformative exhibits security industry organizations can display, if their constituency still does not operate off of a common data strategy or operating framework. Finally, it doesn't matter how transformative vendors become, if their end-users ultimately remain intuitive, reactive threat practitioners who operate in bureaucratic silos only to deliver security outcomes.

The point is that as long as an imbalance in the adoption of digital transformation in the security ecosystem, individual advancements will only put a dent in industry progress. Any ecosystem not actively working in a state of homeostasis is surely at risk.

The fate of the industry doesn't just rely on individual or even collective advancement; it largely depends on whether todays existing ecosystem even sticks together in the long run.

Digital transformation is not only forcing the fate of security companies - who stays and who goes, but it is also requiring the industry to redefine what that business is and who gets to deliver that business. Because digital transformation democratizes data and sensors, it inherently allows consumption by any tech savvy practitioner not necessarily tied to security. Therefore, traditional pockets of the industry are quickly being displaced by more data-driven, non-security alternatives ready to deliver maximum business value. Unfortunately, this is happening all around traditional security players today without them knowing about it.

For example, physical security end-users are quickly losing turf, budget, and accountability to their cyber-security and IT counterparts. Just look at the growing number of CISOs managing physical security for example. Security alarm companies are also being acquired by commercial and residential automation counterparts who plan to squeeze greater business value out of sensors like cameras and door contact points. Traditional systems integrators who stay in their comfort zone of pulling cable or hanging hardware, are being displaced by low-voltage installers who bundle this work into larger jobs, etc. While these are only a few examples, it is very clear that not only are traditional participants feeling competitive pressures, but even transformative players are sensing the friction created in the market. Given these new challenges the physical security industry will become increasingly dysfunctional unless its ecosystem collectively rises to the challenge and gets its transformative act together.

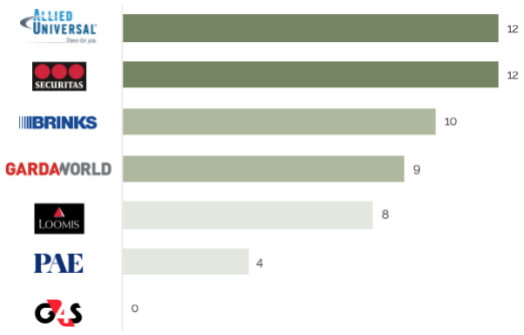
The future of the physical security market heavily depends on a more urgent and collective form of ecosystem engagement, alignment, and orchestration.

Immediate industry wide changes have become more and more operant and will be necessary to avoid overall market erosion. For instance, they need to address with great immediacy the need to technically upskill its security end-user workforce. They need to influence end-user CHROs to hire security leaders based on their technical prowess rather than their prestigious government titles. They need to build industry consensus around data driven priorities like risk frameworks, digital transformation maturity modeling, and success criteria, so that the entire ecosystem can operate off of a common playbook. The physical security industry needs to seek actuarial assistance in building a contemporary security risk model and press insurers to offer premium incentives to end-users that demonstrate real-time, data-driven risk treatment. It needs to lobby its brilliant manufacturing corps to build open-architected systems so that the entire ecosystem can tag-team defeating stagnation. It needs to influence its critical integrator and consultancy base into assuming a stronger value proposition that meets today's end-user and vendor realities. And it needs to offer mission-oriented investors a mutually beneficial scorecard that measures potential impact of their investments toward advancing or disrupting the market ecosystem.

These priorities admittedly will take a lot of work, and more importantly, leadership. The good news is that there is already a strong foundation on which to build well needed momentum. There are pockets of tremendous individual accomplishments by brilliant security leaders all around the industry. There is also terrific precedence of ecosystem engagement to serve as an exemplar, such as global response operators working with insurers, or vendors hosting end-user summits. These efforts need to happen across the whole ecosystem and with greater urgency toward growing a data-centric industry.

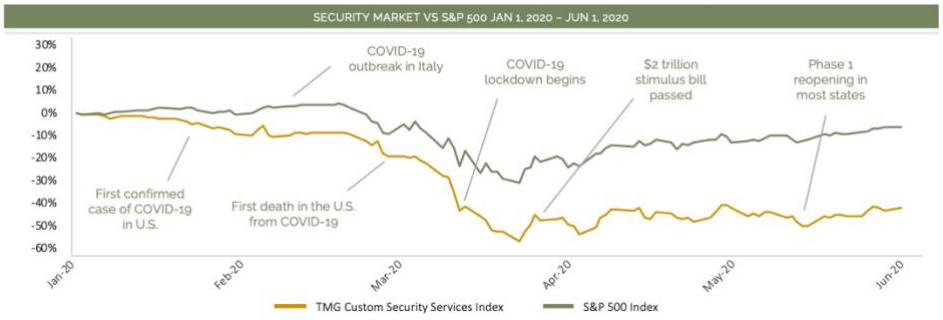
Similarly, the industry's most important quality is also just the right ingredient to get the job done. The security market is largely defined by a hard-working, tightly knit brother and sisterhood of professionals bound by an ethos of selfless service. While alone these common traits will not only help the industry overcome the trials and tribulations of digital transformation, they can enable a call to action and unify the industry toward a more successful tomorrow.

Top Strategic Acquirors 2017-2020



Physical Security Commentary

- Commercial industries have remained security services' largest revenue source, followed by government/NGOs, retail, and residential (chronologically)
- Aggressive M&A activity since 2014 has centered around large strategics' (PLCs and equity-backed) goal of consolidation in effort to gain national/global or vertical footholds, as well as provide a "one-stop-shop" unified protective and systems integration services
- The services industry remains very fragmented, with the four largest players accounting for 21.2% of market share, but with a limited pool of "mid-tier" companies
- The 2024 outlook for security services was positive given corporate expenditure patterns, pace of new business formations, government outsourcing trends, and significant growth in the number of incidents at large public events
- However, COVID abruptly halted this momentum as businesses shuttered, government/corporations went on furlough, and transformative technical advancements became forcedly mainstream (health assurance products, people tracking, etc.)
- Expect competition to grow significantly from technical alternatives such as remote guarding, security-as-a-service, home/building automation, and systems integration



Physical Security M&A Trends

- General upward trend for consolidation over last 18 years, with an increasing share of the industry slowly being dominated by large multinational strategics
- Foreign-owned companies are expected to continue to acquire smaller domestic operators to gain greater foothold in U.S. markets
- Private equity interest in the industry, seeing exit opportunities among large services companies with re-occurring customer base and strong cash flow
- Expectation among end-users for companies to bring additional value, pushing for services to diversify offerings and show differentiation
- Growing trend among large services companies is to consolidate with technology companies to show differentiation and reduce labor costs of guard force
- M&A volume and value of security services companies are at a current low due to COVID-19 but are expected to increase through 2021
- Expect small to medium sized companies enduring weakened financial status due to COVID-19 to seek a merger or acquisition

Marc Gruzenski
Senior Managing Director
mgruzenski@mcleanllc.com
Direct 703.827.0246
Main 703.827.0200

www.mcleanllc.com
7918 Jones Branch Drive, #750
McLean, VA 22102