brivo

SURVEY RESULTS: DIGITAL TRANSFORMATION IN PHYSICAL SECURITY THROUGH CLOUD ADOPTION

INTRODUCTION

During the fourth quarter of 2018, Brivo, in collaboration with Security Management Magazine, conducted their second annual survey of Security leaders from predominantly large multi-location organizations[(1)] to identify 2019 goals and challenges they will face, as well as needs, impacts and barriers to adopting new, transformational technologies.

Respondents provided insight into a range of functional categories to ensure that diverse perspectives are represented in the study results. In this paper, we share the results of our survey, and discuss why Digital Transformation is a major element in the evolution of physical security systems.

Three trends emerged from the survey that we will cover in this paper: The growing importance of moving to a cloud-based model to ensure physical security; the need to integrate mobility and mobile data; and finally, the requirement to take advantage of physical security data to generate insights into organizational effectiveness and customer behavior. These trends point to an overarching phenomenon that is redefining the tech industry: Digital Transformation.

THE POWER OF DIGITAL TRANSFORMATION

It's called Digital Transformation (DX), and it's flipping the business world on its head. Technology, once seen as a tool for mundane, day-to-day, transactional tasks, is now a strategic, transformational, competitive weapon—a business imperative. It has become the tool that facilitates business transformation. Who would have thought that 'cute little projects' like Uber, Airbnb, and Fiverr, perfect examples of Digital Transformation at its best, would bring entire industries to their knees? Or that it would have a profound impact on the physical security industry?

The power behind DX derives from four interrelated elements: organizational collaboration; trust; the power of knowledge-sharing; and the effective use of technology as a business enabler.

Digital Transformation is fundamentally based on an ecosystem of technologies that together allow companies to disrupt, rather than be disrupted. They include cloud and cloud-based services, the Internet of Things, Big Data and Analytics, mobility in all its many forms. Taken together, these technologies form the vanguard for radical business transformation and unassailable competitive advantage.

Digital transformation isn't a thing; it's not a product, or a service, or a technological solution. It's a philosophy—a way to think about how to transform business, using sophisticated digital tools.

TREND #1: THE MOVE TO CLOUD

The global public cloud market is expected to exceed $200 billion[(2)] by 2020, with the vast majority of enterprises using some form of cloud-based service. Added to the already impressive list of as-a-service options (storage, compute, infrastructure, network, etc.) is access control, which, expected to grow at a 15% annual rate[(3)], combines the need for physical security with the power of the converged cloud.

Most organizations are challenged by the fact that they have security data scattered across systems that are logically and geographically dispersed. The only way to achieve data integration across these systems at a reasonable cost and with real-time accessibility is via a cloud-based infrastructure. Data that is available across the entire enterprise leads to higher levels of organizational engagement and collaboration, greater trust, far more effective use of customer data, and solid executive buy-in because of the results that accrue.

Furthermore, survey respondents that have made the jump to cloud widely cite two major benefits: convenience, and increased productivity from the elimination of repetitive, costly, time-consuming tasks like server management and maintenance. As a result, the enterprise embraces cloud and rejects the task and toil of legacy systems.

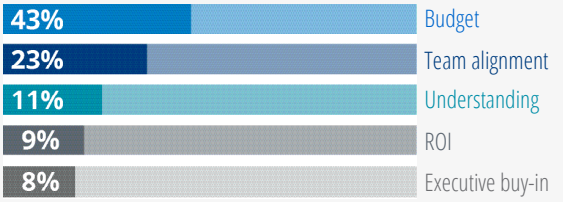
Let's be clear: Most organizations see the move to cloud as a technology decision, when in fact, it's a business decision. Organizations focused largely on the technology aspect of cloud miss the bigger message: that cloud is a force for transformation. Cloud reduces overall IT cost and frees up personnel, allowing the enterprise to focus less on transactional IT management and more on transformation IT strategy, and, as one executive noted, 'If you're not in the business of running a data center, why are you running a data center? 'By moving individual and geographically-dispersed security monitoring and management systems to a shared platform, security organizations can take advantage of the synergy that results.

One manifestation of that synergy is collaborative problem-solving and, by extension, faster, more effective responses to intrusion attempts. And when that happens, the challenge of securing executive buy-in, and therefore, budget, is minimized.

"If you're not in the business of running a data center, why are you running a data center?"

SURVEY RESULTS: CHALLENGES AND BARRIERS TO CLOUD ADOPTION

Our survey participants identified several critical challenges as security professionals: Lack of executive buy-in; limited organizational collaboration; and the ongoing threat of security breaches.
These challenges are also reflected in barriers to adopting new technology which include lack of budget, perceived lack of ROI, no executive buy-in, lack of understanding and lack of alignment This demonstrates a tactical approach on their part, rather than a strategic one.



This is even more relevant when we consider another set of results that the study yielded. When asked what their key physical security goals were for 2019, respondents listed three:

- The integration of physical security systems (access control, video monitoring and alarm);
- The integration of the security organization with other functional areas of the organization, to take advantage of cross-organizational knowledge and insight; and
- A desire to derive value from the data that a converged, cloud-based system generates.

In their book *Blown to Bits: How the New Economics of Information Transforms Strategy,* Philip Evan and Thomas Wurster said, " Far more dangerous than legacy assets is a legacy mindset." Those organizations that fail to heed the evolution of technology will rapidly fall prey to complacency. There is good news on this front: the Brivo study reveals that more than 76% of those interviewed have adopted some advanced technology already, while another 19% are considering their options.

Far more dangerous than legacy assets is a legacy mindset.

Blown to Bits, Phillip Evan and Thomas Wurster

TREND #2: MOBILE INTEGRATION

For most organizations, mobility isn't a technology option—it's a work and lifestyle choice. No surprise, then, that Brivo's study reveals that 81% of business leaders rely on mobile applications to manage their organizations. Multiple studies have shown that a properly executed mobility strategy improves workforce productivity and leads to business growth through always-on connectivity and the deployment of new, innovative capabilities. For that to happen, however, the organization must:

- Clearly define its desired goals
- Deliver a seamless user experience through the deployment of proper APIs
- Focus on information management rather on mobile device management
- Have a clearly thought-out, end-to-end security strategy.

For organizations with a mobile workforce, physical security extends beyond the confines of the workplace, especially for those organizations that increasingly rely on mobile credentials to control access. Given that the average employee is far more likely to forget their access card than they are their mobile phone, the integration of mobile credentialing into the mobile device makes sense for everybody—and provides higher levels of management and control. And, while only 25 percent of our survey participants have adopted mobile credentials to date, barriers to adoption—including a lack of Bluetooth compatible readers, privacy concerns, and IT platform and operating system integration—are disappearing, making mobile credentials more accessible to more security professionals in the future.

MOBILITY STRATEGY

Define goals

Leverage APIs for seamless UX

Information management. vs mobile device management.

End-end security strategy

TREND #3: DATA EMPOWERMENT

Former Hewlett-Packard CEO Lew Platt once quipped, 'If only HP knew what HP knows, we'd be three times more productive.' In the world of today's data-driven enterprise, Lew Platt's estimate is probably off by a factor of ten. Owning the data and having access to the data, however, are two very different things.

Only 36 percent of Brivo's survey respondents reported having a centralized platform supporting multiple locations. Translation? Organizations with security systems scattered across multiple platforms, which tend to be local, only have access to local information. They can't develop a unified data management strategy, because they don't have unified data. Since data can quickly be distilled into insight, and insight is far more actionable and monetizable than raw data, these organizations are at a serious disadvantage.

But the challenges don't revolve purely around monetizability. When a breach occurs, it is critically important to act quickly. It is difficult to respond speedily when the data that must be analyzed lies scattered across multiple systems. Furthermore, there is duplication of effort and infrastructure—not to mention the inevitability of error duplication. Even physical access is adversely affected when multiple systems are involved: employees moving from one physical location to another may find that their credentials are invalid, when single-system credential management, combined with mobility, could eliminate the problem entirely.

This concept of the 'single pane of glass' through which the entire security technoscape can be viewed represents a critical competitive advantage, particularly when we take into account its ability to underpin the delivery of a superior customer experience.

If only HP knew what HP knows, we'd be three times more productive.

Hewlett Packard CEO Lew Platt

FINAL THOUGHTS

Several related trends are causing the business world to shape-shift. Employees and customers are becoming increasingly mobile, and that mobility generates massive volumes of actionable data. Companies struggle to take advantage of that data to provide a superior experience to their stakeholders, and physical security is no exception. Mobile devices generate significant amounts of data that, when examined and acted upon, lends itself to a superior customer experience. But it's one thing to protect a physical facility; it's another thing entirely to protect an employee's mobile device and the data it generates—extensions of the network and data center—when they are on the move.

Equally challenging is the fact that many organizations run multiple, regionally-focused security management systems. These systems operate independently of one another, each generating user data. But because data is the currency of business today, the more that data can be combined across all functions of the organization, the more insight it generates—insight that is not only actionable, but also monetizable. As one survey participant noted, "It's not about getting data, but about getting useful business intelligence. Years ago, your car told you that you would soon run out of gas, because the arrow pointed to the red area of the fuel gauge. Today, it tells you that you have 42 miles of fuel remaining."

Data consolidation means insight consolidation—that's Digital Transformation, and that's the power of the cloud in physical security management.

It's not about getting data, but about getting useful business intelligence. Years ago, your car told you that you would soon run out of gas, because the arrow pointed to the red area of the fuel gauge. Today, it tells you that you have 42 miles of fuel remaining.

ABOUT STEVEN SHEPARD

Dr. Steven Shepard is the founder of the Shepard Communications Group in Williston, Vermont. A professional author, photographer, audio producer, and educator with more than 35 years of experience in the technology industry, he has written more than 80 books and hundreds of articles on a wide range of topics.

He has also consulted, written and photographed in more than 90 countries, serving clients across many different industries.

Footnotes:

1. Participants in the survey included 733 U.S.-based Security leaders—Practitioners, Managers, Directors, and senior executives across a broad range of industries. 79% of those polled were from large, multi-location organizations; the rest managed single-site operations. 68% averaged 50 or more employees per site.
2. Source: https://www.gartner.com/en/newsroom/press-releases/2018-09-12-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2019
3. Source: IHS 2018 Market Projection

ABOUT BRIVO

Brivo is the leader and innovator of cloud physical security for commercial buildings. Currently serving over 15 million users, Brivo provides a centralized cloud-based security management system, including access control, video surveillance, alarms and numerous third-party integrations to its customers. As a SaaS company Brivo aims to provide a convenient and mobile-first approach to securing buildings. Headquartered in Bethesda, MD, Brivo was founded in 1999.

HOW CAN BRIVO HELP YOUR ORGANIZATION?

brivo®
simply better security

Schedule a Demo