WHITE PAPER

An Analysis of the Access Control Industry in Latin America

A study of Latin American end users conducted by HID Global finds that corporations in the area have a pressing imperative to update their access control systems, increase their protection levels, and supplement them with new functionalities.

EXECUTIVE SUMMARY

Physical access control systems are no longer simple tools that authorize or prevent a person from entering a building. Nowadays, these solutions integrate new technologies that provide advanced security and can be applied in a variety of corporate settings.

Despite this, many organizations still do not have plans to modernize their access control systems. This lack of a plan exposes them to many vulnerabilities in today's environment.

Investing in a modern access control system is an important business decision. As such, it is important to take advantage of these systems' maximum potential.

Each of these points was taken into consideration in an HID Global® survey of end users from a variety of Latin American vertical markets. As part of the survey, participants discussed the technology that they currently use for access control.

The results, compiled in this paper, prove that many organizations are still using outdated legacy technology that doesn't provide the protection they need.

In contrast, the current market offers many modern alternatives that are based on high security standards and are within any user's reach, debunking the idea that only large organizations can afford these types of solutions.

Keeping in mind that security is vital to an organization's success, the information in this paper is now available for those companies that are looking to take their security to the next level.

INTRODUCTION

Imagine this scenario: in the 1970s, a well-known car brand launches a new model with exceptional features for its time. Its levels of comfort, performance and safety stand out within the industry. In 2018, these automobiles remain in circulation, fulfilling the basic function of passenger transport. However, they don't meet current safety standards, and customers are dissatisfied with the performance of these vehicles. Would customers consider them a good value? Would they feel safe driving them? Simply put, the answer to these questions is "no." The automobile industry continually produces vehicles with new features and innovations to ensure that their products not only merely transport humans, but also provide superior comfort and safety. Constant innovation ensures that a company is actively meeting challenges as needs change in the industry. To do any less exposes end users to unnecessary risk.

In the Latin American market for physical access control solutions, something similar is occurring. As many organizations maintain their use of outdated tools, they find themselves in one (or more) of the following three scenarios:

1) They continue to operate with insecure systems.

2) They employ obsolete solutions.

3) They fail to utilize capabilities that advanced access control applications offer.

The results of an HID Global survey of 648 security employees in Latin American countries support the above findings. Among those surveyed, 29% were security consultants, 22% were managers or directors of security departments, and 17% were IT managers, directors or other critical personnel. In summary, 67% of those surveyed fall within the category of decision makers in their respective companies, specifically in regards to access control systems.

(All participants were end users within vertical markets such as Construction, General Services, Information, Education, Government and Finance.)

A more detailed discussion of the three scenarios mentioned above follows.

Entrusting Security to Vulnerable Solutions

In this study, 37.3% of participants confirmed that the current technology utilized by their organizations for physical access control are low-frequency cards operating at a bandwidth of 125kHz.

This low-frequency technology entered the market more than 25 years ago, and, despite offering significant advantages in terms of longevity, these identity cards can be easily cloned—often without detection by the authorized user. Moreover, a cloned card can open any corresponding pre-configured door.

Currently, there is no efficient way to determine that a system has been compromised, which provides a false sense of security. Given that a cloned card is perceived as legitimate, any unauthorized person could enter a business's building and use their equipment or services.

According to survey-takers, barcodes make up the second most-implemented security technology, at 20.4%. This finding is disturbing, especially considering that barcodes are the least secure credential technology in use in today's market. Despite being a widespread system in locations such as libraries and supermarkets, barcodes are not effective in terms of security because their main protective element is directly visible, making them extremely vulnerable to copying and other attacks. Considering how simple it is to take a photo of an ID and create a copy of the original—especially in light of the fact that most people in the world own smartphones with high-resolution cameras—compromising a system becomes an easy task.

The third most popular access control technology is the magnetic stripe, used by 20.1% of survey respondents. Even the slow moving banking industry is eliminating this insecure technology, replacing it with 'chip' contact reading. Magstripe cards store and collect information on thin magnetic strips that tend to wear with each use. Even more concerning, analysts maintain that there is no security tied to this technology since the collected data lacks encryption.

On a positive note, 18.5% of respondents indicated that their organizations use mobile access as a form of identification and entrance control. Even if this security form is not yet the most popular in the security industry today, it is gaining recognition for its usage benefits and solid protection against potential intrusions.

Utilizing outdated PACS technologies exposes an organization to the risk of employees' fraudulent duplication and usage of copied cards, opening it to the possibility of unauthorized individuals entering its facilities or—worse—accessing IT and network systems, creating a very severe threat for organizations.

In some cases, employees might copy ID access cards to enter an organization's system and steal information under another colleague's name. Unfortunately, it is all too easy to copy and transfer information from one proximity card to another—there are even video tutorials on YouTube that offer instructions.

Exploring New Options

It is clear that the primary purpose of physical access control solutions is to allow only authorized individuals into any given building. However, these tools can also offer additional benefits that aren't currently being explored or utilized by the majority of end users.

The HID Global study found that the authentication system feature most often used by respondents is physical access control alone (75%). Considering this statistic, it is important to note that PACS solutions can be applied to other use cases—especially those that survey participants mentioned separately.

Additional applications of access control cards depend on user type. For example, in a mid-market residential community, the security solution at hand is expected to keep condominium doors closed and parking gates down. However, in a premium market area, this same solution can also be configured to control the pool, spa and communal zones. These integrated services become possible when the systems use powerful smartcard technology with integrations among various software elements.

In business cases, access cards are an employee's main form of identification and also provide implicit services. Depending on the organization's software, this same ID card can be used to provide food vouchers or manage the company's printing system.

The possibilities are limitless when it comes to linking access control systems to additional services, constrained only by the creativity of an organization's staff. For example, it is possible to control the privacy of printed documents within the organization, verify that the department utilizing printing services is paying for them, register transactions, manage vending machines and more with an access control card.

All of the necessary information is already included on the specific card, which encrypts data that is then recognized by its readers.

Using Old Data Technology Results in Dissatisfaction

Another element addressed by HID Global's analysis relates to the age and support available for existing access control solutions. It is vital that end users know the age of existing products and services as it relates to their system's complete lifecycle. Moreover, if a solution has a known vulnerability, is not supported, or has no replacement parts readily available, it should be updated as soon as possible.

According to the survey results, 11% of respondents currently utilize card readers that were introduced more than six years ago. This timeframe also applies to software (9.4%), controllers (11.4%), and cards (9.8%) that are currently in use.

The use of outdated solutions has a direct impact on the satisfaction levels of end users: approximately 46.4% of participants said that they had conformed to the use of an access control tool that did not even satisfy their basic or expected requirements.

On this note, it is necessary to underscore the importance of security professionals' ability to stay up-to-date with access control technologies and trends. While it is a harsh reality that businesses don't always have the financial resources to update their tools, it is essential for decision makers to remain familiar with new options on the market.

Despite these sobering facts, there are still end users who do not have plans to update elements of their security systems in the near future. Specifically, 23.6% of survey respondents affirmed that they had not considered the possibility of modernizing their readers, ID cards, controllers or software.

Outdated Access Control in Latin America

It's no secret that the regional security situation is a considerable worry for governments and businesses, not to mention local citizens. As a result, it has been necessary to identify and adopt more advanced methods of protection.

A prime example of this necessity originated in 2018 in the region of Recoleta, an area in Buenos Aires, Argentina. In this case, authorities worked to capture a group of criminals who were consistently replicating coded keys to local residential buildings. These 125 kHz keys were a prime target because they had been created in 1990. According to Argentine media[1], over fifty break-ins had occurred in approximately six months by the end of 2018.

These coded keys can be easily copied by criminals with a digital device purchased easily online. The copy is processed in about five seconds and generally costs $1.14. In this specific case, the Argentinian community elected to introduce several "anti-hacking"[2] devices that prevent a building door from opening when prompted by a copied key.

To prevent situations like these, manufacturers like HID and its network of certified partners recommend updating technology to include the most recently released generation of devices, which use cryptographic elements that prevent duplication.Furthermore, these experts recommend using keys with top encryption, such as those offered by HID Global®, which are very difficult to clone.[3]

---

[1] América Noticias (2018, September 6). América Noticias nos visita para saber sobre llaveros electrónicos.
Found at: https://www.youtube.com/watch?v=PaZc9av8gRs

[2] A24 (2018, September 6). ¿Llaveros electrónicos clonables?
Found at: https://www.youtube.com/watch?v=Mo5JFpBFxNU

[3] A24 (2018, September 2016). Entrevista en vivo con América 24 por los llaveros electrónicos.
Found at: https://www.youtube.com/watch?v=L1_pHAoRTLE

HOW CAN THE ENVIRONMENT IN LATIN AMERICA BE CHANGED?

Unfortunately, Latin American end users continue to cling to outdated technologies that are more than 20 years old, which generate sizable security gaps.

As an example, some end users believe that video surveillance cameras provide enough security to detect and prevent any possible risk. However, this assumption is far from reality. In Latin America, it is common to find highly vulnerable and susceptible security environments like these that have originated from end users' lack of awareness in regards to access control.

When these clients are prompted to update their technologies and tools, many respond like this:

- "My identification system still works."
- "The tool I'm using has a lifetime guarantee."
- "I don't have the time to learn and introduce better industry practices."
- "Having to change the setup or protocol in my shopping system is a very complex process."
- "Manufacturers are only suggesting this for their gain."
- "I don't have the budget for it."

In an attempt to protect themselves, organizations in the Latin American market have supported solutions that—while they were suitable in their time—have fallen short of the region's current security needs.

First generation cards are a prime example of one of these solutions. Originating in the 1990s, they operate at a low frequency of 125 kHz and run a high risk of duplication fraud.

Second generation cards, which appeared in the market between 1996 and 2002, offer a higher level of protection thanks to the inclusion of a memory chip, but are still at a high risk for duplication.

Third generation cards, released in 2011, operate at a higher frequency of 13.56 Mhz and include a Secure Identity Object (SIO) or broadly equivalent technology. The latter is a data model that allows only one specific object's identification data to be stored and transferred. As a result, it is often used in access control devices such as name tags. While these cards are much more secure, it is worth mentioning that they still run the risk of replication.

In 2014, the latest generation of security technology emerged, bringing with it Seos® credential technology. This powerful, innovative solution for secure identification works exceptionally well in the realm of access control. One of Seos' most significant benefits is that it provides secure access to more applications while allowing the final user to utilize whichever device that they prefer—all while providing total user privacy.

Other advantages include:

- Flexibility in physical or virtual identification card implementation
- A much lower per-card price point in comparison with Prox
- Long- and short-term security
- Functionality across many applications
- Mobile access control support

Since 2017, businesses have begun to perform updates, primarily because they have had more resources with which to conduct them. Unfortunately, the same does not apply to many small and medium-sized businesses, which have not had the same level of capital to make these investments.

Even though more end users realize the risk inherent to their situation, investment in such updates has been relatively low. If order for these projects to make a global impact and affect various countries in the area, the designation of a significant budget is key. This is in addition to the establishment of security as a business priority.

MODERN SOLUTIONS: ALTERNATIVES THAT CAN CHANGE THE CURRENT SETTING

It is impossible to discuss modern access control solutions without referencing the technology that makes each of these innovative new tools possible: Seos. Available for physical and digital credentials, Seos is designed to be highly portable.

This portability means that Seos can appear on a physical card or a mobile device, as well as on other devices such as smartwatches. Seos is a platform that enables stronger security while providing the convenience of a constantly evolving access control solution.

Considering the rate of daily cell phone theft in Latin America, however, it is clear that security conditions throughout the region present a central challenge to mobile access control systems. Despite the substantial benefits that Seos brings to the table, doubts inevitably arise when considering the outcome of a lost or stolen phone. How does one disconnect the system from the device itself so that another individual cannot use the attached credentials?

Addressing this concern, experts reassure that, just like physical nametags, virtual nametags only work if their corresponding systems authorize them to access a restricted area. Thus, with HID Mobile Access, a system administrator can immediately remove any associated authorizations granted to an employee in the event that they lose their phone or leave the organization.

It is evident that these modern technologies are positive for many businesses, not only due to the enhanced security they provide, but also because they are not expensive or complicated to introduce. Seos card readers, for example, can easily be adjusted to accept specific credentials so that the end user is prepared and ready to go almost immediately.

Technological Updates Accessible to Everyone

Small and medium-sized businesses might very well assume that this range of specific, modern technologies is only intended for and accessible to larger organizations. What options does a company with limited staff and a small operation have, especially if their current access control solution is not dependable, and they want to adopt something more trustworthy, efficient and secure? Considering these points, the solution should be difficult to duplicate and available at a reasonable price point.

The answer to these concerns can be found in modern access control solutions, some of which don't require a costly investment and aren't accompanied by the expectations of other solutions known for maximum quality. These two characteristics alone surpass most conventional security tools.

A related concern is Return on Investment (ROI) and the potential profits earned from implementing such an update (or new system overall). HID experts explain that it is difficult to achieve precision when calculating ROI on solutions focused exclusively on credentials due to project variance. While some solution updates might include simple card readjustments, others might require distinct additions that cost extra. In this case, pricing is similar and doesn't necessarily signify a huge change, since a simple review of each application's details is enough to detect any differences at hand. Thus, from an ROI perspective, potential variance originates in the cost differences between applications.

That being said, the price of an unauthorized individual gaining access to and copying information from corporate credentials is one that would be very difficult to estimate. In this case, the individual could enter wherever and whenever they desire. Imagine if this occurred in a company that manages highly confidential information or inventory. How much could this breach cost the organization? What is the price of ensuring that no one enters a building to threaten or harm its staff? Fortunately, each of these situations can be avoided through the use of security tools like mobile credentials.

On the other hand, managing and processing physical identification cards also incurs other costs, such as those stemming from printing and distribution. Some companies end up spending significant amounts of money to send cards to remote employees. Upon comparing these costs to the possible savings gained by using new technologies, it is easy to conclude that these modern access control tools are much more financially efficient. A combination of physical and digital identification methods is also a feasible option, thanks to these new systems.

Expanding Beyond Physical Security Methods

In contrast to the opinions of many end users, access control does not merely protect the physical premises. This misconception is due to a lack of consideration of the potential vulnerabilities of an organization lacking the necessary security. Further, it doesn't take into account that the user experience itself has changed.

Mobile solutions have significantly changed this scene, as they have uncovered previous tools' security vulnerabilities and shortcomings. They streamline for IT directors the enormous responsibility of managing not only desktop computers, but also server and cloud-based applications. IT must now guarantee access, monitor video, and ensure physical security while also protecting against possible intrusions. As a result, the security landscape has changed—so must access control.

On this note, it is important for security professionals to consider all possible weaknesses and insecurities, whether they pertain to IT or physical threats.

CONCLUSION

Before the Internet, it was possible to depend on relatively secure technology, given the fact that most people did not know how to break into security systems. Because no method of information transfer as efficient as the Internet was in existence, it was the age of "security through obscurity."

Now, with so many different ways to access information via the Internet,,malicious individuals can easily infringe upon a business's physical and logistical security. Add to this the availability of relatively affordable cloning resources, and the gravity of the situation is clear.

So, why run the risk? The information and technology needed to increase organizational security is not only available but within reach for everyone. The risks are a reality, and identity fraud is regularly accomplished, thanks to large virtual stores and outlets. The greater the danger, the larger the consequences suffered by the end user.

On this note, protection should not be limited to the physical setting alone, but should also extend across the entire building technology spectrum. A company's failure to do so would be the equivalent of running a business on Windows 3.0, the popular version of the Windows operating system released in 1990.

Security and privacy are extremely important to end users. As a result, organizations of all sizes should remain aware and up-to-date on news and trends about physical and logistical access. HID's mobile access solutions are available for any sized company—including those who think they cannot afford a new access control system,or weren't planning to modernize their existing solution.

2019-04-29-hid-pacs-lam-acc-crtl-ind-lam-wp-en

PLT-04414