FINANCIAL INSTITUTIONS REQUIRE FUTURE-READY PHYSICAL SECURITY TECHNOLOGIES TO MITIGATE RISK, INCREASE CUSTOMER CONVENIENCE AND ENHANCE TRUST
With rapidly increasing competition, financial institutions are looking for new technologies that help them innovate their workplace experience, increase customer convenience and differentiate from competitors. This rapid innovation means financial institutions now face unprecedented threats to their image and reputation from security attacks that may be launched at any time across their organization, from their main headquarters to each of their individual branch offices.

Often highlighted as one of the most dangerous of these threats is a major data breach; however, reputational risk extends further to include anything banks do—or don’t do—that leads customers to lose confidence in the trustworthiness of their transactions and how their personal information is being protected. A critical line of defense in addressing these concerns is physical security. “In today’s connected environments, overlooked building systems can serve as an entry point for cyberattacks and physical ‘brute force’ attacks designed to take advantage of previously unknown vulnerabilities,” said Ian Lowe, Director of Product Marketing at HID Global.

As a result, today’s physical security technologies are a key factor in shoring up a financial institution’s image as an innovative, trustworthy and forward-looking service provider.

An Increasingly Challenging Threat Landscape

Financial institutions are laser-focused on avoiding reputational damage. Eighty-seven percent of executives surveyed in a recent Deloitte study stated that this threat category is “more important” or “much more important” than any other strategic risks their companies face. Mitigating these risks has become even more difficult in recent years. The banking and financial services industry is at the center of disruptive changes that have created new and even more challenging vulnerabilities while shifting how consumers regard security and trust.

Customers are driving this disruption as they demand ease of use and a better banking experience. “In a global digital marketplace, customers are free to choose the financial institutions that cater most effectively to their needs. The winners are those that can deliver purely digital experiences that streamline customer workflows and provide an intuitive interface for engagement that leads to higher levels of satisfaction. This includes meeting a growing preference for mobile experiences and self-service banking,” Lowe said.

Accommodating customers’ needs requires a corresponding shift in the business model for financial services. For instance, growing demand for simplification in the digital world filters down to the bank-building experience in the physical world. At the same time, the move to mobile pushes institutions to reduce their overall physical footprint and remove walls, so they can drive efficiency and innovation in a world where real estate is increasingly at a premium.

Financial institutions must respond to these disruptions by strengthening defenses, not only via their IT systems, but also on the equally important physical security side where they must control access and have a high level of location awareness of people in their buildings. “One step in any breach or attack may be through someone gaining unauthorized physical access to a bank’s branch, headquarters or other facility. Another step could include attacking the physical security hardware that is connected to the network or the cloud,” Lowe said.
Evolving regulatory enforcement acknowledges the importance of physical security as well. For instance, the Small-Entity Compliance Guide published by the United States’ Federal Reserve includes an overview of the Gramm-Leach-Bliley Act (GLB Act) security guidelines for physical safeguards which ensure the security, confidentiality, integrity and proper disposal of customer information. These safeguards include measures for permitting access only to authorized individuals at physical locations containing customer information, such as buildings, computer facilities and records storage facilities.

“One step in any breach or attack may be through someone gaining unauthorized physical access to a bank’s branch, headquarters or other facility.”

The European Union’s General Data Protection Regulation (GDPR) also impacts the physical space. As customers and employees interact with smarter buildings, they leave a digital footprint and create the potential for misuse of personal data. GDPR has mandated numerous requirements related to how data must be stored and for how long, among other directives.

There are many examples of wide-reaching data breaches where attackers first exploited a physical security vulnerability to gain access. Such was the case with the infamous Sony Pictures hack, which was reportedly the work of a criminal who gained unauthorized physical access to the corporate network with help from someone on the inside. More recently, an attempted breach at Medrobotics in Massachusetts involved a visitor who somehow made it through the facility’s physical security checkpoints and spent more than two hours with on-site access to the guest network. It wasn’t until the CEO noticed the intruder sitting in a conference room, which was behind the company’s security perimeter, that the culprit was questioned and discovered.

Even when both IT and physical security are robust, there may be cracks between the two systems that sophisticated attackers can exploit using cross-platform techniques. This is especially true as financial institutions become more connected. Indeed, while most may have invested heavily in physical and network security to protect against traditional threats, the greatest threats may come from vulnerabilities associated with devices connected to the Internet of Things (IoT), including video surveillance cameras and both physical and IT security systems. It’s critical that financial institutions address these vulnerabilities; this will likely require actionable data analytics across both IT and physical security so that financial organizations are able to effectively predict and identify threats in real time.

These and other challenges have raised expectations for physical security as an integral piece of a unified risk-mitigation strategy.

**New Expectations for Physical Security**

A survey by HID Global of more than 1,500 IT Managers, Directors and staff, as well as Chief Information and Chief Technology Officers, reveals how perceptions about physical security have changed.
Which of the following features would you most require in a new physical access control system? Select all that apply

- Easy to use: 71%
- Ability to add or support new technologies in the future: 68%
- Mobile access (ability to use smartphones, tablets, wearables for access control): 59%
- Integration with existing security platforms: 54%
- Support for more advanced and higher security features: 53%
- Open-standards-based technology for easy integration: 52%
- Support by existing service providers: 33%
- Innovative future roadmap from product manufacturer: 26%
- High-quality warranty and extended support services: 5%
- Other: 3%


Among the findings was a trend toward greater collaboration between physical and IT security teams as roles change and technologies converge on corporate networks, in the cloud, and with IoT. The survey found that IT departments are now more involved than ever in an organization’s physical access control decisions and implementation. More than half (55 percent) of respondents reported IT as primarily responsible or having shared responsibility for access control within their organization. As a result, IT leaders are tasked with spearheading not only the protection of their company’s network—and cybersecurity-related initiatives—but also those set forth by the physical security department to protect employees, visitors, and assets from internal and external threats.

Similarly, the study showed that the IT department will increasingly play a role in physical security to influence technology decisions (76 percent) through the integration of access control within the ecosystem (72 percent), by implementing access control technology (59 percent), and through the management of access control systems (39 percent). The top pain point identified by respondents was that physical access control systems were not integrated with other IT systems (50 percent).

The study also revealed a future-focused perspective among respondents. This is echoed in EY’s Global Banking Outlook 2018 report that called for banks to complete the transition from regulatory-driven transformation to innovation-led change, so they can successfully insulate themselves against the impacts of future downturns on financial performance and business continuity.

Likewise, results of the HID Global study reveal a perception that physical access control system success depends on the ability to prevent unauthorized individuals from accessing network-related hardware as well as the ability to easily add emerging technology options.
The top five features that respondents said they would require in a new access control system were:

1. Easy to use (71 percent)
2. Ability to add or support new technologies in the future (68 percent)
3. Mobile access, or the ability to use smartphones, tablets, wearables for access control (59 percent)
4. Integration with existing security platforms (54 percent)
5. Support for more advanced and higher security features (53 percent)

“Organizations are also moving away from vulnerable legacy-proximity technology to smart/multi-technology ID credentials that can store and authenticate biographical information, PIN codes or currency for vending using standardized encryption techniques.”

**Legacy Technologies Give Way to More Advanced Solutions**

Coming in a close sixth on the feature list was open standards-based technology that ensures easy integration (52 percent). Migrating to standards-based technologies also results in a more secure and future-proofed access control system.

One of the most prominent examples of the industry’s move away from legacy technologies has been the transition from Wiegand to the OSDP standard with Secure Channel Protocol (SCP), which supports both IP communications and point-to-point serial interfaces such as RS-485. As a co-inventor, HID Global is one of the first to support OSDP with SCP in its iCLASS SE® reader portfolio, improving security and lowering costs while enabling interoperability and stimulating systems integration.

“Organizations are also moving away from vulnerable legacy-proximity technology to smart/multi-technology ID credentials that can store and authenticate biographical information, PIN codes or currency for vending using standardized encryption techniques,” Lowe explained. For example, recent breakthroughs in credential technology now provide advanced security and authentication capabilities along with the ability to extend the use of a single credential beyond physical access control. “In essence, solutions such as HID Global’s Seos® credential technology enable physical access control systems to become the backbone for streamlining security through a financial institution,” Lowe added. Physical access control, network log-in, secure print, and many other authentication and enterprise access control capabilities can be consolidated into a single, trusted and far more secure ID. Because these solutions are software-based and independent of the underlying hardware chip, they also provide new levels of form factor flexibility, including use on mobile devices for authentication—a rising trend in financial and other smart enterprise environments.

Additionally, with the move to smarter buildings and the drive to innovate the employee and guest workplace experience, organizations are adding sensor technologies to their buildings, assets and occupancy management ecosystems. These sensors include the Bluetooth Low Energy (BLE) sensors in location services which enable organizations to deliver new experiences like room-level, real-time occupancy views, wayfinding and automated/personalized building environmental controls.
Pillars for Successful Risk Mitigation

Among the physical access features that organizations have shortlisted as they look to the future, two are particularly important for mitigating the challenging security risks faced by today’s financial institutions: the ability to provision mobile IDs to employees’ smartphones and location services.

Going Mobile

Mobile IDs have the potential to fundamentally change how banks operate. They give employees the convenience of using their smartphones, tablets or wearable devices to do everything from accessing doors, gates and networks to opening electronic locks, securely releasing documents from the printer, purchasing snacks from the vending machine, and “punching in” to time and attendance systems. Available as a stand-alone capability or integral feature of an existing card-based system, solutions like HID Mobile Access make it easy to manage employee access rights while taking advantage of automated flows that increase administrative efficiency for issuing and revoking mobile IDs. Powered by Seos, HID Mobile Access delivers best-in-class cryptography for unrivaled data and privacy protection for access control. This also simplifies compliance to major privacy frameworks, such as GDPR and Privacy Shield, by ensuring that no personally identifiable information or financial data is stored.

By 2020, Gartner Inc. estimates that 20 percent of physical access control solutions will be shaped by mobile technology and cloud architectures.

Location Services to Improve Governance and Situational Awareness

Location services offer similarly transformative opportunities by enhancing area governance. This enables institutions to improve visibility and situational awareness so they can ensure safety while protecting critical assets. As Lowe explained, "Combining IoT technologies with predictive analytics, today’s location services solutions enable financial institutions to improve real-time visibility through knowing the precise location of items, employees and visitors. Employees benefit from the ability to locate needed assets, and institutions gain valuable knowledge about building occupancy and employee location so they can facilitate evacuations and emergency responses, while also meeting requirements related to access policies, time-and-attendance logging and building safety." Precise real-time and proximity location capabilities make it significantly easier to manage who enters and exits the building, and to control where, when and why they can access specific areas and information resources.
The Connected Security Ecosystem

Adding mobile access control and location services to standards-based physical access control infrastructures gives financial institutions a solid foundation for incorporating other valuable risk-mitigation capabilities while enabling innovations in workplace experience. For instance, biometrics adds the ability to unequivocally validate a person's identity for greater security and convenience, without adding complexity for the employee or customer. Personal Identity Verification (PIV) solutions can also be a valuable addition, giving banks an integrated solution for standards-compliant identity and credential management with the ability to use a single secure credential for accessing facilities and IT resources. An example is HID Global's PIV Enterprise™ multi-factor authentication solution, which encompasses the entire identity lifecycle—from identity proofing and secure credential issuance through retirement of the trusted secure credential. HID Global also offers PIV enablement solutions that permit financial institutions to meet any assurance level as defined by the federal government.

Two other capabilities that should be considered include visitor management and cloud-based ID card printing. Visitor management solutions such as HID's EasyLobby offer automated guest management, which makes it easier for banks to meet compliance mandates related to collecting and auditing visitor data. To improve ID card issuance for visitors, as well as employees and contractors, banks have the option of adding cloud-based ID card printing. Solutions like HID FARGO Connect combine all aspects of the issuance process and cloud-based services into an easily scalable ID badging solution that removes the expense and labor associated with managing ID personalization/issuance through a local computer. All data is transmitted using end-to-end
encryption that meets banking-level protocols, giving bank administrators the confidence to adopt a cloud-based technology that reduces badging costs while also providing full visibility and control through a more efficient issuance process.

By 2020, Gartner Inc. estimates that 20 percent of physical access control solutions will be shaped by mobile technology and cloud architectures. In the future, physical access control readers, controllers, panels and locks will also have the ability to be connected to the cloud. This will deliver valuable new risk-mitigation benefits, along with opportunities to further enhance efficiency and user convenience. Cloud-based monitoring applications will bring access control systems into the advanced smart building solution set and deliver analytics capabilities for proactively pinpointing and troubleshooting potential system failures. The applications will also monitor secure connections between access control peripherals and trigger firmware updates to address potential cyber threats.

**Future-Ready Security Posture**

Financial institutions need robust physical security solutions to protect their people, properties and assets. They also need these solutions to help minimize reputational risk by simplifying regulatory compliance while plugging vulnerability gaps in today’s increasingly connected banking environment. These solutions “must also enhance the organization’s credibility as a forward-looking service provider that creates high-quality workplace experiences for its employees and innovative new options for customer engagement and service delivery,” said Lowe. These challenges can be solved by building a physical access control solution on a standards-based foundation and adding key technology pillars including mobile access and location services. Putting these technologies into employees’ hands enables banks to visibly demonstrate a current and future-ready security posture, which gives customers and employees a deeper level of confidence and trust.

Learn how your financial institution can create a multi-layered security strategy that protects your buildings, networks, and systems. Visit hidglobal.com/access-control.