

News

Banking security: A closer look at the Vanderbilt playbook



As prime targets for criminals, banks have always faced major security challenges. But today, when banks are pressed to increase revenues, improve operational efficiency, and mitigate risk, defending against security threats is increasingly expensive. Two key drivers in the banking sector are customer trust and operational efficiency. Both are significantly strengthened by a quality integrated 'smart' banking security solution.

A robust security strategy is of the highest priority and is usually embedded within the bank's Risk Management Plan. This enables banks to manage operational risk and compliance demands. The modern approach to bank security design incorporates IT, Channel Management and Identity and Access Management systems into one solution.

At the heart of Vanderbilt, systems is compliance with some of the highest industry and regulatory standards. These systems impact all bank functions and help deliver greater trust, operational efficiencies, and excellent customer experience.



Playbook

In the bank's self-service area, Vanderbilt can provide live video surveillance that continuously monitors and provides quality images should a suspicious event need to be investigated.

Meanwhile, Vanderbilt's Seismic detectors protect ATM's 24/7. These detectors give immediate and reliable alerts of attacks on the enclosure, but unlike other detectors, do not register false alarms triggered by passing traffic or the vibrations of the ATM itself.

Electronic security measures are also used in other banking situations – for example, when a customer claims he tried to withdraw cash from an ATM and was issued a receipt, but no cash – the bank can check with a specialized data department to ascertain whether the money was deducted from the customer's account.



Unique codes grant workers who fill ATMs access to secured areas and the ability to unlock ATM's. The worker's code over-rides any 'delayed unlock function,' so he can immediately access the ATM and fill it. There are set time limits for the work to be done. The ATM buzzes for a pre-determined time before the machine is due to auto-lock. If the worker needs more time, he can delay this. Once the job is done – the ATM automatically locks.

Interlocking

Another example of bank security involves interlocking. When a staff member unlocks the vault, the door to the secured area simultaneously locks. This prevents anyone else from gaining entry until the vault is once again locked. This ensures the safety of staff members and the security of vault contents.

There are many layers of electronic security protecting the bank. If the manager arrives early, he uses his card to gain access to the branch office and a PIN to disarm the alarm. His code disables the office and secure area, but the ATM's, vaults and safe deposit boxes remain armed. A Central Monitoring Station is alerted to the early entry. They need to know whether the entry is routine or under duress. The monitoring station views the manager on live video as he executes a pre-determined security procedure and until he hits an 'All is OK' button. If there is a problem – the manager can send a silent 'Duress Alarm' rather than

the 'All is OK.' The Monitoring Station can listen in – and if necessary can call the police.



Security in banking is an essential issue. It requires thoughtful attention and procedure while allowing room for agility, adaptability, and dependability – flagship traits of the Vanderbilt brand. Banks wish to operate in an open and friendly layout while ultimately safeguarding their customers, staff, and assets. Vanderbilt's solutions respond to these expectations and enable active safeguarding foundations to be laid.

[#ReadyForAnyChallenge](#)



vanderbiltindustries.com