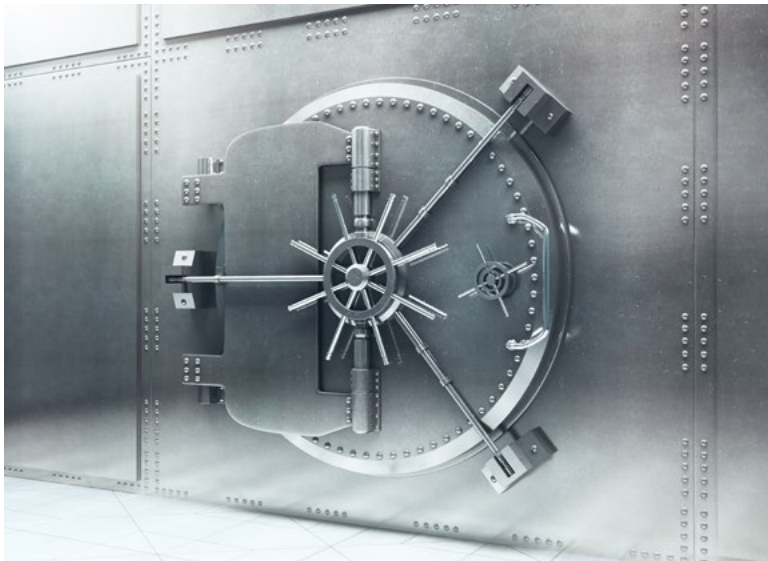
VANDERBILT

Protecting Financial and Banking Institutions: Trends, Considerations and Planning

As prime targets for criminals, banks and financial institutions have always faced major security challenges. The market is constantly evolving to meet the growing demands of customers for convenience and enhanced service, while balancing the considerations necessary to protect these same people from outside risks — both physical and cyber.

As banks are pressed to increase revenues, improve operational efficiency and mitigate risk, defending against security threats is paramount to the success of the market. The rise of fraud in many financial institutions requires security directors to incorporate robust strategies for mitigating its emergence. According to the 2017 American Bankers Association Deposit Account Fraud Survey, fraud against bank deposit accounts cost the industry approximately $2.2 billion in losses in 2016.



Data protection in the modern era is also a challenge for today's financial institutions, as guidelines like the General Data Protection Regulation (GDPR) in Europe signify a shift toward increased privacy, affecting virtually every company working in the financial sector. Collaboration between both security and IT departments, as well as the incorporation of cybersecurity into the development of access control, intrusion and video management solutions, brings both physical and cybersecurity to the forefront of risk management strategies in the financial sector. Building a solid foundation using these as a guide can modernize and streamline the protection of this market.

This white paper will explore the emerging risk management and security trends in the financial sector, as well as considerations that must be made when formulating a comprehensive safety and security plan.

5 EMERGING RISK MANAGEMENT AND SECURITY TRENDS IN BANKING

With the rise in cyber attacks at the forefront of the news on a near daily basis, it's becoming increasingly clear that the role of risk management and security must be elevated throughout the financial services and banking markets. Physical and IT security leaders are shifting toward a more proactive approach to security than in years' past to address and mitigate the latest emerging trends.

1 Security Breaches

Cybersecurity or data breaches can cost organizations millions of dollars, not to mention the loss of trust in the brand by consumers looking to them to protect their critical information. This is especially true in the financial services realm. In 2017, a ring of hackers called the Carbanak gang was discovered by the Kaspersky Lab, where it was reported the ring had stolen more than $1 billion from financial institutions around the globe.

As a result, more and more financial institutions are focusing their efforts on both physical and cyber security. Gartner reports that worldwide information security spending will reach $93 billion this year, while Cybersecurity Ventures predicts global spending on cybersecurity products and services will exceed $1 trillion leading up to 2021 — and this is just the beginning. As hackers become more sophisticated,

so too should the security measures in place to thwart attacks. This includes increased spending on products that engage in constant vulnerability testing, bringing all stakeholders to the table to collaborate on solutions, and introducing innovative technology that helps mitigate fraud.in place to thwart attacks. This includes increased spending on products that engage in constant vulnerability testing, bringing all stakeholders to the table to collaborate on solutions, and introducing innovative technology that helps mitigate fraud.

2 New Regulations

Regulations have a significant impact on how businesses manage data and security — especially in the financial sector — and data can be both an asset and a potential liability. The GDPR, a European effort to regulate how entities that do business with people protect their private information, provides a new set of data privacy rules far more extensive than ever seen before. It's a complicated implementation that security leaders must look at carefully to ensure business continuity and compliance.

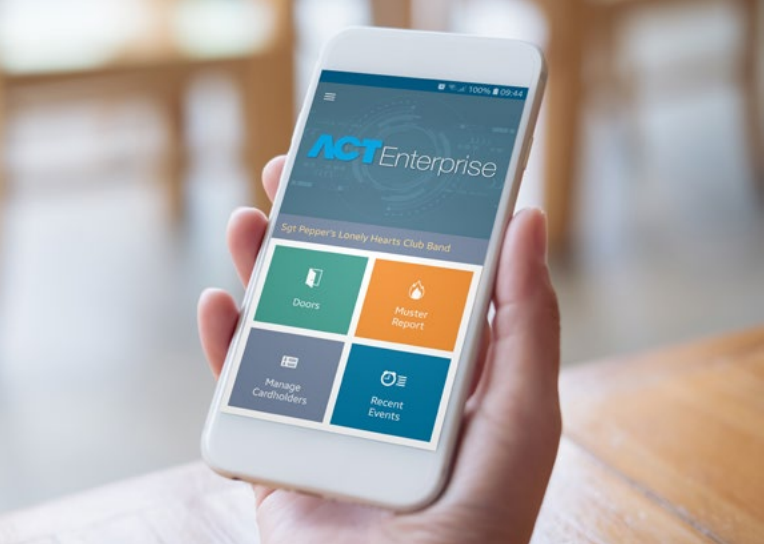
Whether located in the European Union (EU) or simply processing the data of subjects residing in the EU, financial institutions find themselves at the center of this legislation. Banks must work diligently to comply with the GDPR to avoid penalties that can reach up

to 4 percent of the company's entire global revenue. Additionally, users and installers must seek out vendors that understand the implications of the GDPR and its potential impact on security systems that store and access sensitive data.

3 Cloud-based Solutions

Forward-thinking financial organizations are undergoing a seismic shift away from legacy systems toward new and emerging technologies, such as cloud-based solutions. Cisco predicts that by 2020, global cloud use will account for more than 92 percent of total data center traffic. This surge in adoption also represents a huge uptake in spending, which Gartner predicts will exceed $1 trillion in purchases dedicated to the cloud by 2020.

The cloud can deliver more agility and scalability for growing organizations, which can be ideal in the banking industry as satellite ATMs and new branches are added to a security plan. More and more businesses realize that leveraging the cloud is the most efficient way to solve emerging challenges. Today's cloud-based technology can empower financial organizations to take a more proactive approach to security management, allowing information gathered about people and vehicle movement, for example, to be readily available and actionable for security leaders. Cloud-based solutions can deliver a range of advantages including greater security, more resilience, ease of mobile user support, flexibility, reduced costs and a greater user experience.



4 Remote Monitoring Capabilities

Modern technology has resulted in a society that is always connected. For the security industry, this means it is now possible to remotely monitor many locations from hundreds of miles away. Cloud-based solutions provide a unique advantage for security directors to streamline security system management and maintenance from anywhere at any time, managing multiple locations seamlessly from a unified interface.

Remote monitoring is a backbone feature of many solutions on the market today, allowing unparalleled flexibility for security directors to act quickly and efficiently in the event of a breach or emergency. This ability allows for the elimination of once laborious tasks, such as reporting, that are now available through the quick click of a button on mobile or desktop devices. Essentially, remote monitoring provides ease of use and convenience, which can be critical for today's financial institutions and the security leaders that help protect them.

5 Fraud Mitigation

For a bank or credit union, the emergence of fraud and the amount of money lost to this threat is increasingly significant. As criminals become more sophisticated, financial institutions have to identify the best way to use time and money in an effort to mitigate the risk of fraudulent activity in their facilities.

The first step is bringing video surveillance and data management solutions together to integrate fully with access control and intrusion, creating a comprehensive approach to addressing emerging threats.

NAVIGATING INTEGRAL SOLUTIONS FOR BANKING SECURITY

A robust security strategy is of the highest priority and is usually embedded within a bank's risk management strategy, which enables banks to manage operational risk and compliance demands. A modern, multilayer approach to financial institution security incorporates IT, video, intrusion, identity and access management systems in a comprehensive solution that serves to protect people, assets and the brand.

Video Surveillance and Management

Video surveillance footage, when incorporated into a video management system (VMS) that can detect, record, analyze and deter threats to personnel and assets within a facility, is paramount to the success of any security team within a financial institution. Today's VMS solutions can incorporate both legacy analog cameras and IP solutions as part of an evolving integrated security management solution.

Video is a critical part of a financial institution's security plan, providing essential oversight into the day-to-day operations of bank or credit union. Specifically, in the bank's self-service area, cameras can provide live video surveillance that continuously monitors and provides quality images should a suspicious event need to be investigated.

ATM Seismic Sensing, Protection and Vault Interlocking

Seismic detectors protect ATMs 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. They have been developed for false alarm immunity and even the subtlest attacks can be detected at a very early stage, repeatedly triggering an alarm that gives ample time for intervention.

Unique codes grant workers who fill ATMs access to secured areas and the ability to unlock them. The worker's code overrides any "delayed unlock function," so he or she 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.

Another example of bank security involves interlocking. When a staff member unlocks a 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.

Monitoring Safety

Central monitoring stations (CMS) or security operations centers (SOC) can work quickly and correctly to identify the source of any alarms. As a direct consequence, the number of needless callouts due to false alarms can be significantly reduced. For example, a manager arrives

early and uses his or her card to gain access to the branch office and a PIN to disarm the alarm. His or her code disables the office and secure area, but the ATMs, vaults and safe deposit boxes remain armed.

A CMS or SOC is alerted to the early entry and they need to know whether the entry is routine or under duress. The monitoring station views the manager on live video as he or she executes a pre-determined security procedure until the manager 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" communication. The CMS can listen in and if necessary can call the police.

Personal Security Devices

Personal security devices increase the confidence and security of bank employees, while also offering a set of specifically defined "financial" area types for ATM and vault environments with pre-defined times and enhanced security functions. Users can define the period during which an ATM or vault remains unset. Once that period expires, the ATM or vault automatically sets to an interlock group, thus denying further access to other ATMs or vaults if any area within a group is unset.

Central Database Monitoring

Many banking institutions have hundreds if not thousands of locations to manage and maintain, as well as provide security oversight. Checking the activities and frequency of service providers, as well as monitoring the technical performance of the system is a challenge and requires a huge administrative effort.

A networked solution can remotely monitor the sites and collect valuable data on a regular basis. With a central database approach and extensive data mining from a number of sources, financial institutions are able to supervise and automate the distribution of reporting/trending information to the necessary stakeholders with minimal efforts.

MULTILAYER APPROACH

The above solutions, along with various departments and operational processes, must come together to form a comprehensive security plan to meet the evolving and demanding needs of the financial sector.

Information Sharing and Collaboration.

Information sharing is crucial in today's data-driven environment. Improved sharing allows financial organizations to easily communicate information across multiple locations, which can help officials detect known criminals and recognize patterns of fraud. By taking a collaborative approach, these organizations are able to minimize risks that are inherent in more siloed systems and locations.

For example, IT departments are already well-versed in the ins and outs of a company's computers, network and software, and they share a common goal with physical security teams of protecting critical data and keeping outsiders out. A strong relationship with IT professionals is invaluable when it comes to achieving the maximum safety possible for a bank's security network.

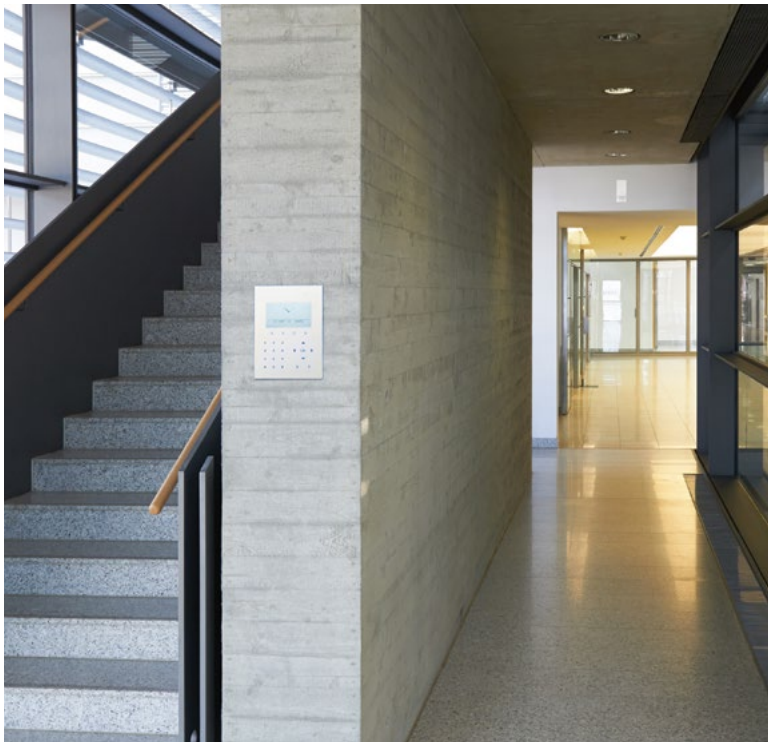
Financial institutions must also keep in mind creating a strong relationship with public entities, such as police and fire departments. Streamlined and open communication with these organizations can go a long way in providing the necessary teamwork required to achieve thorough protection and immediate response in the event of an incident.

ACHIEVING COHESIVE SECURITY FOR THE FUTURE

Complex threats to data, privacy and physical assets can greatly affect a financial institution's bottom line and result in loss of both money and trust for consumers. It

is a central mission for these organizations to achieve the highest level of security today and in the future by utilizing new technology, features and strategies for risk management and mitigation.

Vanderbilt intrusion, access control and video management solutions provide robust technology aimed at helping financial institutions meet their goals of becoming safer and more dedicated to protecting customers from internal and external threats. Vanderbilt offers end-to-end solutions, from detection point to alarm receiver, from a single technical partner. These solutions can be configured and customized to cost-effectively meet the needs of small to large banking and financial installations. Coupled with collaboration between departments and outside agencies, these solutions can go a long way in providing the peace of mind needed for financial security leaders in today's threat landscape.



Banking on Robust Solutions: Case Studies

BANCA DI CESENA E BANCA DI GATTEO CREDITO COOPERATIVO S.COOP

Solution: Vanderbilt SPC Connect, SPC5000 and SPC6000 control panels

Italy's Credito Cooperativo (BCC) consortium of banks are found throughout the length and breadth of the country and have served local communities for the past 134 years. There are 317 mutual not-for-profit organizations comprising over 4,300 branches, all of which work together to guarantee a range of products in keeping with the values and identity of a cooperative.

Headquartered in Cesena, Banca di Cesena e Banca di GATTEO Credito Cooperativo S.Coop is the first member of the BCC to initiate a new security infrastructure. The bank wanted a system that offered integration between access control and intrusion detection as well as being reliable, easy to install and future proof.

Highlights:

- Vanderbilt's SPC is a true hybrid intrusion detection system that meets EN 50131 standards and has unmatched flexibility and scalability.
- The control panels are fully integrated with Vanderbilt's pioneering SPC Connect system – a cloud-based solution that allows Smart Security to monitor, manage and control the SPC control panels remotely from any location.
- SPC Connect offers the ability to customize how data is viewed by setting up a feature that allows Smart Security to manage and control access rights to individual panels and groups of panels. This means that tasks such as configuration management, troubleshooting and regular maintenance can be carried out remotely, saving massive amounts of time and money, and enabling a swift resolution to any issues.

BANK PEKAO

Solution: SiPass, SPC panels

Bank Pekao is a Polish financial institution considered to be one of the safest banks at the pan-European level that operates almost 1,000 branches, the second largest network in the country.

The bank wanted to move toward an IP based solution that could centrally monitor, maintain and control different branch offices around Poland to allow more efficient management. This would mean that any issues could be identified immediately and remedial action could be taken when necessary.

Highlights:

- SiPass integrated is a powerful access control system that provides security without compromising convenience and ease of use. SiPass integrated is a part of Bank Pekao's system that restricts movement within each branch.
- Bank Pekao also required full interoperability between the SPC panels and access control systems for operations such as arm/disarm area, alarm notifications and input/output status readings.
- This level of high-end operability means that the entire system is run over a single network that can be centrally managed, allowing it to work smoothly and ensuring maximum security for all bank branches.
- It also provides an open interface for any third-party software, offering the possibility to integrate access control with other systems – therefore creating one intelligent building management solution that can check the status of doors, prompt the Vectis video recorders to activate and provide a full audit trail.

Vanderbilt Banking Security Products:

SPC Connect • ACT Enterprise • SiPass integrated • Vectis iX

About Vanderbilt

Vanderbilt is a global provider of security systems recognized for future-proof, high-performance, easy-to-use products. Vanderbilt strives for innovation in Software-as-a-Service solutions such as **ACT365** and **SPC Connect**, as well as product integration both within and outside of their portfolio offerings. Simply put, Vanderbilt is **#ReadyForAnyChallenge.** To learn more, please visit **vanderbiltindustries.com**, or follow us on **Twitter**, **Facebook**, and **LinkedIn**.

For more information, please contact:

Ross Wilks

Head of Communications

+44 2036 300 695

rosswilks@vanderbiltindustries.com

VANDERBILT

vanderbiltindustries.com

@VanderbiltInd Vanderbilt Industries

Vanderbilt International Ltd.

Clonshaugh Business and Technology Park

Clonshaugh, Dublin D17 KV 84, Ireland

+353 1 437 2560