



Creating Trust.

WINCOR
NIXDORF



Patrick K., with a high level of criminal energy

“You know where your bank’s weak points lie?
– I do!”

„Almost half (44 %) of the incurred data loss expenses related to the cost of lost business, reflecting the added expense of consumer churn and the increased difficulty of attracting new customers in the wake of negative publicity.”

Source: Ponemon Institute/PGP Corporation: 2009 Annual Study: Global Cost of a Data Breach, Understanding Financial Impact, Customer Turnover and Preventive Solutions. Menlo Park/Traverse City, 2010.

The banking sector pays a high price for the criminal energy of anonymous lawbreakers who put their knowledge about bank vulnerability to very successful use. The effect is always the same, irrespective of whether the crimes involve skimming attacks or safe-breaking. Banks suffer not only financial damage but also a major loss of confidence among their customers and partners – very serious consequences indeed, especially if you consider the fact that almost half of the incurred data loss expenses are caused by lost business.

The risks facing your bank include active attacks such as the classic bank robbery at gunpoint, safe-breaking with explosives, ram raid, intrusion and vandalism. Increasingly, physical attacks are taking on a modern form, with card trapping, cash trapping and cash reversal fraud just some of the highly alarming methods currently in use. Unfortunately, their logical counterpart in the shape of viruses, trojans and worms also continues to make negative news.

In addition to this, passive processes also generate risks: theft of sensitive data are just one example of such methods.

The last risk group involves hazards that are caused unintentionally, primarily as a result of errors made by bank staff themselves. However, it also includes environmental influences and natural catastrophes such as fires and flooding.

Hazards are therefore generated from a range of different sources but it is internal and external attacks launched by criminals that account for most of the threats to banking environments. The very nature of banking business itself presents numerous dangers: the great attraction of cash and the existence of sensitive information is today transforming banks into high-risk enterprises.

If banks fail to install vital protective measures, hazards can soon become serious risks. In order to guarantee business continuity, satisfy customers and win back lost trust, it is vital that they keep pace with the latest developments. It is becoming increasingly important to control risks, above all in times of great uncertainty. Regrettably, protective measures tend to be ignored until concrete economic loss is imminent – by which time it is often too late!

State-of-the-art risk management – a must have in banking business.





Three steps to an all-in-one solution.

State-of-the-art risk management with ProTect from Wincor Nixdorf equips you to close security gaps long before any damage is caused and, in doing so, to minimize your overall risk.

ProTect is an all-in security concept that covers the entire risk management process. We help you through all steps, from risk analysis and risk minimization to risk control, thereby ensuring that potential damage is kept to an absolute minimum.

Three process steps are all you need to launch protective measures that equip you to manage risks on a holistic basis. They transform a scenario full of potential risks into a far less hazardous environment, and do so with minimum interruption to your work. You benefit from maximum protection that keeps your institution's assets safe over the long term. Because, of course, all four assets that need protecting – your bank's brand, people's lives and health, cash and information, and investments – will all affect your financial situation if they are not looked after properly. Opt to benefit now from the optimized security that ProTect offers as the unique selling and differentiating feature for your bank's success!

■ Step I: Risk analysis

During the first step of cooperation, our consultants collect the information they need to obtain an overview of the current risk situation at your bank. This ensures that they can design and implement the perfect solution for your financial institution.

This step gives top priority to inventorying your bank's assets. "Which assets and processes actually need protecting?" – this question must be answered as precisely as possible. Our consultants analyze the entire range of business processes in your company, its infrastructure, the hardware and software it uses, information, application data, communication links and, of course, the roles and work environment of each member of your staff.

The results of this basic analysis are then classified. Corporate assets and processes are grouped according to their individual protection needs. Conceivable threats are identified and assigned a probability and an estimate of the possible damage they could cause. This systematic and methodical analysis of the present situation in your bank reveals and records risks right at the start of your project.

The next task is to define the areas that most urgently need protecting and to recommend customized protection measures. At this stage, the measures that will be applied are naturally chosen in line with your bank's risk

policy.

Since it is essential to guarantee legal compliance, diverse security regulations must be taken into account. These include the following legal, regulatory and similar requirements as well as specific industry standards, all of which apply to providers of financial services:

- German control and transparency in companies law (KontraG), German banking act (KWG), German stock corporation law (AktG)
- MaRisk and SOX
- PCI, EMV, SEPA
- Data protection act and rules for avoiding counterfeit money
- Occupational safety law, e.g. Germany's UVV Kassen
- Central credit reference agency (ZKA), German Federal Supervisory Authority for Financial Services (BaFin)
- ISO, ANSI

ProTect risk management adheres to the security guidelines laid down in the IT Baseline Protection Manual, Common Criteria and the international Information Security Standard ISO/IEC 27001.

Best-in-class security consulting is a key component of the overall concept. This service from Wincor Nixdorf's consultants ensures that ProTect provides active security that spans all the business processes in your bank.

The first step: detailed analysis & end-to-end evaluation.



The second step: systematic fulfillment & active implementation.



ProTect minimizes risks, providing solutions for

- ... identification and access control for customers, employees, cash-in-transit operators and technicians
- ... cash security throughout the entire cash cycle
- ... data and software security to ensure confidentiality, integrity and availability
- ... continuous security monitoring that provides for reliable control

■ **Step II: Risk minimization**

The second process step is about minimizing risks, in other words active implementation of the jointly developed security concept. At this stage, individual security measures and solutions are implemented in your bank.

Wincor Nixdorf's phased concept comprising prevention, detection and correction solutions offers all-in protection for security in your institution. The vast array of information and advice supplied by our security consultants supports you in implementing the right security solution that establishes the optimal balance between protection and cost-effectiveness. Finding precisely the right level of security to suit your company is a key criterion on the way to a successful future for your bank.

Perpetual and highly systematic evaluation of all known risk scenarios, market analysis and ongoing further development of our own protection systems puts us in a position to offer you innovative security solutions. – Remember that Wincor Nixdorf was the first ATM manufacturer with an own anti-skimming solution!

■ Step III: Risk control

Controlling and monitoring risks are indispensable components of Wincor Nixdorf's all-in security concept. These are two elements in the third ProTect process step.

During risk control, our staff check whether the protection measures that have been implemented are effective across the board and whether all risks have been minimized. Are all ATMs protected from tampering? Are the building and its equipment sufficiently protected? Does this include all processes and are they secure? Is the entire IT optimally guarded? The risk control step also includes mobilizing all persons involved in this scenario, a step that can be achieved with security and awareness-raising training sessions for bank staff and customers.

The range of topics involved is rounded off by the introduction of contingency plans and ongoing updates that keep security solutions up to date as new risks emerge. Regular audits are a crucial factor: they guarantee cyclic analysis of all your bank processes to ensure compliance with requirements and guidelines and their subsequent re-evaluation.

Risk monitoring represents the third process step. Professional monitoring guarantees seamless surveillance of all the processes in your company. Some examples of features that characterize risk monitoring as a compo-

nent of the ProTect concept are:

- Video surveillance at the ATM as a deterrent and for documentation purposes
- Fraud recognition and forward transfer, enabling smooth resumption of all processes in the wake of an attack and ensuring a high level of business continuity
- Tracing incidents and reactions to guarantee early warnings and permanent audit trail capability

Security experts attest to Wincor Nixdorf's top-class Managed Security Services during the final step of this operational risk management.

As new risks are emerging all the time and criminal energy never peters out, ongoing risk management is absolutely essential. ProTect gives your bank one big advantage; the trust of your customers.

The third step: ongoing controls & seamless monitoring.



Best-in-class protection – for the security of your bank, thanks to ProTect.

Operational risk management from Wincor Nixdorf offers fully comprehensive protection and thus meets the expectations of both your customers and bank's security experts.

Bank customers expect all-in protection against fraud and tampering during their financial transactions. This naturally applies to all delivery channels, for instance cash withdrawal or credit transfer transactions at self-service systems as well as at the bank counter.

Experts at financial institutions who are confronted with security issues on a daily basis emphasize the importance of bank staff safety and optimal protection for the bank's infrastructure and IT equipment. What your bank needs is therefore a harmonized, sustainable solution that establishes comprehensive overall protection for your customers, your staff and your bank.



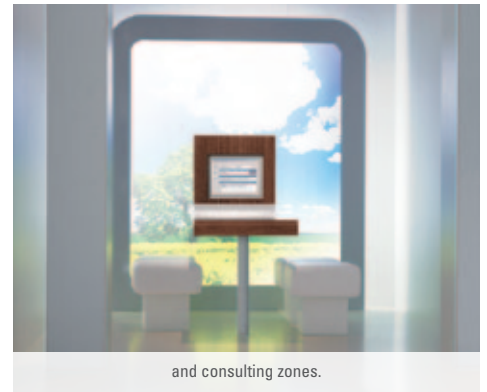
Reliable planning with ProTect: protection for the entire branch, ...



from the self-service zone ...



to the front-office ...



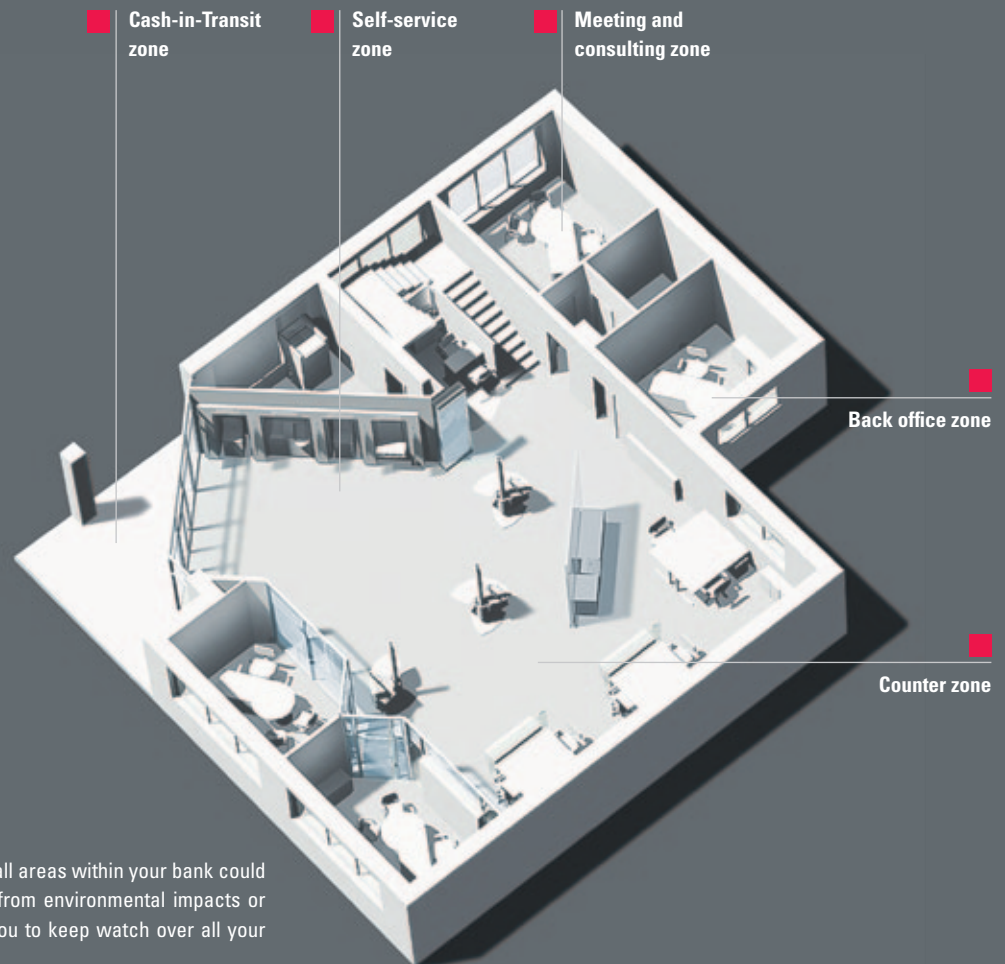
and consulting zones.

Wincor Nixdorf provides full support for your institution with intelligent ProTect security solutions – and does so throughout all the lifecycle phases of your bank branch.

As a full-service provider, we are equipped to provide support right from the start. We draw on our longtime experience as we accompany you through from the planning stage of your construction project to branch opening once this phase is over. Our consultants are also ready to provide support during branch operations and to offer a broad array of solutions when branch renewal is imminent.


All this saves you unnecessary work, avoids extra costs and prevents coordination problems arising. As our customer you therefore benefit from the comprehensive ProTect concept throughout all phases of your security projects.

All sensitive zones under control – right from the start, thanks to ProTect.



Risks for sensitive zones in a bank:

If inadequate protection measures have been installed, all areas within your bank could soon be the scene of criminal attacks, suffer damage from environmental impacts or be jeopardized as a result of human error. – We help you to keep watch over all your sensitive zones.

A man in a dark grey suit, white shirt, and red tie stands in a modern office. He is holding a pair of glasses in his hands. The background shows a conference room with a long table and several chairs, with large windows and indoor plants.

Robert F., bank director

“I am looking for a universal security concept for my bank. – But does such a thing exist?”

Brand ProTecton

One of the most important factors that contribute to bank success is its brand. This valuable asset could be damaged or even destroyed completely by gaps in its security concept. For example, if the name of a bank hits the headlines as a result of its inadequate measures to protect data, this could have a negative impact on the bank's value. This often represents a greater threat than loss of equipment. Your bank's image plays a key role in your success and cannot simply be restored!

Hacker attacks are one of the biggest hazards of our time and represent a major risk for banking business. Illegal access to data, software and networks via viruses, trojans and worms is on the increase. Man-in-the-middle attacks also represent major potential risks and should be prevented by installing an end-to-end security solution. We help you guard your company against these and similar external and internal attacks, to ensure that criminals are not given a single chance.

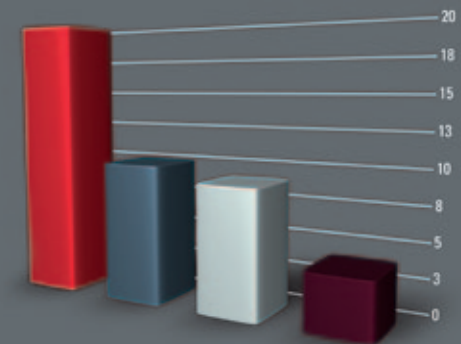
As an experienced security expert, Wincor Nixdorf offers you solutions you can rely on to prevent illegal access to your ATM software. What is more, it makes it virtually impossible to spy out PINs and other data as it passes via the different transmission paths.

Moreover, we have the right answer to problems caused by illegal access to employees' PCs: single sign-on coupled with biometric recognition. This feature ensures that information can be accessed only by employees who have been granted permission to do so and that password cannot be spied out by other people. Our consultants can also help with the assignment of internal privileges to your staff, to ensure that special rights are granted only when special needs exist.

All steps that are conceivably necessary must be taken to ward off damage to your institution. Because, ultimately, if company losses can be traced to inadequate security measures, attention will focus on its executive managers and board members when liability claims are made. Security is not just the responsibility of a specialist department but of the company as a whole!

With ProTect we help you do all that is necessary and appropriate to prevent image loss and to safeguard your company from liability risks. In this way, Wincor Nixdorf protects your bank's brand and generates trust by guaranteeing secure business processes.

Protecting your brand generates trust.



External attacks in 2009:
(Repeated occurrences in %)

- Virus/worm outbreaks
- Loss of data through physical attacks
- External financial fraud using information systems
- External information theft

Most banks are attacked in different ways several times a year. In 2009, more than 20% of all banks worldwide suffered multiple virus and worm attacks!
Source: Deloitte/Touche/Tohmatsu: 2010 Financial Services, Global Security Study, The faceless threat. London, 2010.



Nicole D., bank employee

“I enjoy working in my branch. But I do sometimes get worried about my safety here.”

Life & Health ProTect

The people in charge have to define the most important asset that needs protecting within an end-to-end security strategy: the answer is 'people'. "The lives and health of our customers, staff and business partners must be given full protection at all times!" – a precept that has top priority and must be complied with.

If we take a close look at the latest statistics, we see that attacks on customers are a very common crime. Intrusion, bank robbery and other similar offenses pose a threat to everyone involved – including the bank's own staff. Attention must be focused on the latter for other reasons: they are the key to your company's success but, at the same time, a lack of security awareness among bank staff is the main source of security breaches. Whether these are due to intentional or unintentional errors, the outcome is equally devastating.

Protecting the life and health of your customers, staff and business partners is vital factor if your institution is to be successful: customers who do not feel completely safe will not be your customers much longer. Employees who fear for their health will not work to full capacity. And business partners who do not feel well looked after by your bank will not be overly keen to do business with you.

We use ProTect to help you define optimal protection for all three groups. Here are some examples from the Wincor Nixdorf solution portfolio:

- Security training and timely notification of an alarm protect all the parties in a bank
- Our lobby surveillance feature creates a secure atmosphere for people withdrawing cash
- Other ProTect solutions ensure that bank staff rarely come into contact with large volumes of cash and therefore cannot be coerced into handing it over to criminals

Wincor Nixdorf draws on expertise it has gained from numerous banking solutions all over the globe. We will be happy to share this with you right from the start of your project and to join with you in making your branch a secure place. Should you so require, we will provide support during initial planning for your new bank, design optimal protection and help you implement your individual security system, continuing as your partner long after this phase is over.


We want people to feel safe – at all times.

326 robberies at financial institutions in Germany alone in 2009!

Alarming figures: 326 robberies were recorded at financial institutions in Germany in 2009. This represents a rise in robberies of almost 10%. Almost three-quarters of these attacks were carried out by armed criminals – a shocking résumé!

Source: Federal Criminal Police Office (BKA): Police crime statistics 2009, Wiesbaden 2010





Maria S., bank customer

“I’m used to withdrawing cash from an ATM now. But you read so many reports about card fraud ...”

■ Cash & Information ProTecton

Cash and sensitive information have always been vital components of banking business. Nowadays, however, a secure data stream guarantees the availability, confidentiality and integrity of information where, in the past, a code of honor and handwritten notes were sufficient. Equally important is, of course, a secure uninterrupted cash cycle.

As a multifunction tool, today's ATMs are a key instrument in the provision of banking services. Due to ongoing improvements in mechanical and electronic protection, the downward trend in violent attacks on ATMs continues. However, incidents in which criminals attempt to gain access to customers' bank cards or their data through tampering have soared. Skimming, a method by which criminals spy out a user's card data and PIN, undoubtedly tops the ATM crime charts.

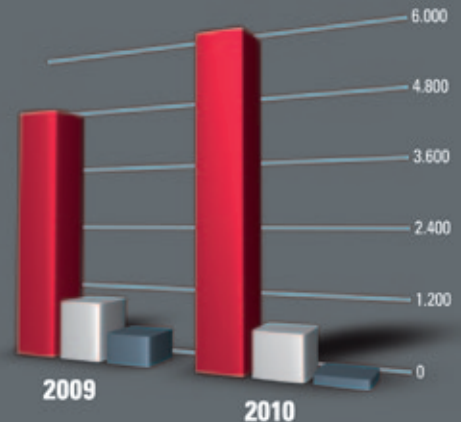
With ProTect, Wincor Nixdorf has established a solution concept that begins with identity and access controls on the system itself: one vital security step is to use intelligent measures as protection against ATM skimming attacks. In addition to security solutions that prevent data being read, further manipulations can be detected via an intelligent surface monitoring solution. What is more, biometric recognition on ATMs helps to prevent all types of card abuse on these machines.

Maximum security is guaranteed by the fact that not only card data and the secret number are verified but that the user's identity is also checked. Additional protection is offered by card readers that retain cards if they detect a card trapping attack. Cameras mounted directly on ATMs are another way of preventing tampering.

ProTect also offers highly efficient protection for the cash cycle: the optimized banknote validation function on automated teller machines, for instance, guarantees top reliability. Alongside many other solutions, software from Wincor Nixdorf delivers added security for bank ATMs by optimizing replenishment volumes and cash holdings.

The complex ProTect solutions comply with data protection regulations as well as with the specific requirements of the Payment Card Industry (PCI) and the European Central Bank (ECB).

ProTect: no chance for ATM tampering!



ATM-related fraud attacks:
(By number of incidents in the first half of the year)

- Skimming attacks
- Card Trapping attacks
- Other fraud attacks

A comparison of the first half of the years 2009 and 2010 reveals startling facts: The number of skimming attacks in Europe has risen once again in 2010. Compared to the same period of time in 2009, the figure has increased by 24%!

Source: Gunn/Lachlan: European ATM Crime Report 2010, Period: January to June, Edinburgh, 2010



Michael P., insurance broker

“I would like to insure a bank
– but just how high is this branch’s
actual risk?”

Investment ProTect

A compulsory condition for the payment of insurance benefits is that your bank has end-to-end security measures installed – since, after all, major assets are involved. This is where ProTect comes in: its bundled security measures mean that the remaining risk can be insured neatly and economically.

Investments are the basis for all business processes and therefore need optimal protection. In addition, it is important to apply appropriate security measures so that you avoid machine downtimes and interruptions in your bank operations – failing to do this could spell high costs. Remember that deficient implementation of security mechanisms could result in a hefty fine!

Experience from the recent past makes one fact absolutely plain: it is often the unspectacular solutions that provide highly effective service in helping to prevent criminal attacks over the long term. For example, the use of cash-staining technology on ATMs has proved to be a major deterrent that results in fewer attacks being carried out on machines. In other words: using intelligent protection mechanisms to prevent attacks and communicating this fact on a broad base will result in fewer crimes being committed in the long term. Deploying preventive technologies therefore helps to minimize overall losses, avoiding the

loss of cash as well as other effects including physical damage to self-service systems and the branch itself.

The following components of an end-to-end security concept are often prerequisites for insurance protection at your bank:

- Protection of equipment used for uninterrupted power supplies
- Use of locks and safes with different security classes
- Intruder alarm systems in ATMs and secure ATM mountings

ATMs from Wincor Nixdorf have passed extensive Association of indemnity insurers (VdS) testing with flying colors and thus meet all the requirements defined in European regulations.

Preventive action with banknote staining solutions:

The intelligent ink-staining system is activated when the ATM's cassettes are removed without authorization, when the ATM is shaken or its position changed, etc. It stains the banknotes with ink, making them completely useless for criminals.

ProTect minimizes risks: both reassuring and cost-effective.



ProTect means one-stop, end-to-end protection.

With support from security expert and global market player Wincor Nixdorf, you know you can rely on a strong partner. Benefit from our longstanding experience in the banking sector to ensure that your security system is a perfect fit for your needs. At the same time, share our ever increasing know-how so that you always have the right response in the event of new attacks!

Wincor Nixdorf consultants subject all persons and processes within your institution to an end-to-end analysis. ProTect caters for all three steps of the risk management process. This gives your institution a state-of-the-art concept that provides your staff and branches, products and processes with comprehensive protection.

ProTect focuses on the key success factors for banks: its brand, people's lives and health, cash and information, and investments. It takes full account of legal, technical, organizational and, of course, personal aspects in order to create a comprehensive security scenario and implement it with proper care. ProTect wards off expected and unexpected difficulties and reduces the likelihood of their occurring.

As our customer you benefit from the all-in ProTect concept throughout all phases of your security project. We provide prompt expert support – during all phases, from planning to

implementation and including support during operations. The proven expertise of specialists at Wincor Nixdorf ensures that you take delivery of your solution on schedule and that all components interact optimally. Finally, when your security equipment is up and running, we provide a full array of services that relieve you of the routine work, and are ready to help if and when critical situations occur – 24 hours a day, 365 days a year. This enables you to focus your full attention on your core business.

ProTect supplies you with optimized protection from a single provider – security for your bank's success.

ProTect



ProTect. Creating Trust.

Profit from ProTect, the all-in concept for active security from Wincor Nixdorf. Let us help you strengthen customer confidence in your financial institution!

Published by
Wincor Nixdorf International GmbH
Heinz-Nixdorf-Ring 1
33106 Paderborn, Germany

Phone +49 (0) 52 51 / 693-33 01
Fax +49 (0) 52 51 / 693-59 18

www.wincor-nixdorf.com

© **Wincor Nixdorf International GmbH**

All product names are registered trademarks of
Wincor Nixdorf International GmbH.
All rights reserved, particularly in relation to the
grant of a patent or the registration of a utility model.
Photo source: KRANZ InnenArchitekten, page 8.
Subject to availability and technical modifications.

Order Nr. R10004-J-Z731-2-7600
Printed in Germany, December 2010