Diebold Nixdorf

2024

Cybersecurity Threat Report

DieboldNixdorf.com

Table of Contents

A Note from the Chief Information Security Officer

Diebold Nixdorf partners —

In the ever-evolving landscape of the digital age, cybersecurity remains at the forefront of global concerns. As the world becomes increasingly interconnected, the banking and retail industries find themselves at the nexus of innovation and vulnerability. Technology's rapid evolution has brought unparalleled opportunities for development and growth. However, it also ushered in a new era of sophisticated threats that can jeopardize not only our organization's integrity but also our customers' trust.

We specifically tailor each edition of our Cybersecurity Threat Report to banking and retail, which have been the primary targets of cyberattacks in recent years. In an era when the digital and physical realms converge more than ever, these sectors play crucial roles in the economic ecosystem. While they empower consumers with convenient financial transactions and seamless shopping experiences, they also handle vast amounts of sensitive data, making them lucrative targets for malicious actors.

Threat intelligence is not merely a concept but a dynamic, proactive approach. Within these pages, you will find insights on cybersecurity, physical security and emerging cyberthreats and forward-thinking methods for staying one step ahead of developing trends. Our team of experts joined forces to offer their combined knowledge and experience as a valuable resource for industry leaders, decision-makers and professionals tasked with safeguarding their businesses, customers and stakeholders.

What can you expect to take away from this document?

1. A comprehensive understanding of the current threat landscape
2. Practical approaches for threat mitigation to safeguard your most valuable assets
3. Strategies for predicting, detecting and responding to adversarial moves in real time

Our collective commitment to the security and resilience of the banking and retail industries drives us as we continue navigating the evolving digital landscape with determination and knowledge. Together, we can fortify our organizations, protect our customers, and ensure the future remains secure for commerce and innovation.

Scott Barronton
Chief Information Security Officer, Diebold Nixdorf

The Importance of Threat Intelligence

Threat intelligence and information exchange should be top priorities for every organization because threat actors talk daily about potential ways to hack infrastructures, systems and companies. Finely tuned advanced intelligence systems can detect risks affecting an organization's overall structure as well as its individual products. This preparation enables the rapid deployment of precise countermeasures to mitigate specific threats, reducing the potential scope and impact of adverse events.

For example, Diebold Nixdorf's surveillance infrastructure is strategically designed to identify emerging tactics that could compromise ATM security and newly developed malware engineered to exploit specific systems. Including surveillance within the intelligence framework allows us to develop defense mechanisms as unique as the threats they neutralize, especially in a security landscape marked by increasingly specialized threats.

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

— Sun Tzu

Proactiveness

Proactively exploring high-risk digital environments, such as the constant surveillance of notorious darknet forums and known malware distribution lists, is integral to any organization's cybersecurity posture and helps maintain an advantage. This approach enables a company to identify emerging risks early and respond quickly with defensive countermeasures.

External Collaboration and Information Exchange

Diebold Nixdorf partners with esteemed entities like BVK Technology, Cardtronics, Europol, GMV, ING, Interpol, KAL, NCR Voyix and TMD Security. Together, we delve into the benefits and challenges of participating in threat intelligence, share platforms and communities specific to the banking industry, and emphasize the value of exchanging intelligence with peer organizations, financial institutions and security vendors.

Threat Intelligence at Diebold Nixdorf

Threat intelligence encompasses the holistic defense of our company and Product & Solution Security-related topics, making it a pivotal force in preserving Diebold Nixdorf's digital integrity. We are dedicated to staying ahead of emerging cybersecurity threats that may target any aspect of our operations. Collecting and analyzing intelligence on potential risks empowers us to make informed decisions, implement proactive security measures and protect our digital assets.

- **Monitoring and Analyzing Threat Intelligence Data**
  Diebold Nixdorf's strategy is forward-thinking, continuously striving to be ahead of potential threats. We employ security technologies to examine unusual digital behaviors. This type of analysis identifies current risks and uses predictive modeling to foresee future threats. As a result, we can strengthen our security posture by successfully applying mitigations before threats can materialize. The aim is to evolve with the ever-changing nature of threats, thereby maintaining robust defenses that successfully avoid risks before they can intensify.

- **Automated Threat Intelligence Platforms**
  Diebold Nixdorf leverages automated threat intelligence platforms (ATIPs), which are crucial in streamlining the threat intelligence process. ATIPs automate the collection, analysis and dissemination of threat data, resulting in faster response times. These platforms can aggregate information from diverse places, such as open-source feeds, forums and incident reports. While the automated nature enhances efficiency, it is important to recognize that relying solely on algorithms may overlook contextual or nuanced threats. Therefore, balancing automation with human expertise is crucial for a comprehensive and effective defense strategy.

- **Information Sharing Platforms**
  Information-sharing platforms tailored to specific industries are critical in proactively addressing emerging threats. Active engagement in these collaborative networks enables the timely exchange of threat intelligence among relevant entities, enhancing the collective defense against cyberthreats.

  Diebold Nixdorf collaborates on industry-specific platforms to facilitate real-time sharing of actionable intelligence related to cyberthreats, vulnerabilities and best practices. Our teams also gain valuable insights from peers, fostering a more comprehensive understanding of evolving risks and threat landscapes specific to their business. This collaborative approach contributes to a more robust defense strategy against emerging challenges.

Product & Solution Security

Product & Solution Security focuses on industry threat intelligence, incident management, loss prevention and security by design as part of Diebold Nixdorf's global Information Security function. Our mission is to protect and shield our customers against the evolving threat landscape of attacks against self-service ecosystems.

Incident Management

- Investigate all attempts to get illegitimate access to cash or information
- Serve as point of contact for customers and Diebold Nixdorf employees, who can report any incident to Security@DieboldNixdorf.com
- Oversee globally binding processes connecting central experts with local representatives in many different countries

Industry Threat Intelligence

- Cooperate with different organizations and law enforcement agencies across the globe
- Contribute to cross-industry standardization of definitions and create white papers
- Analyze underground forums and darknet activities
- Develop threat intelligence for new trends and vulnerabilities

Loss Prevention

- Research customer claims of physical cash losses
- Govern shared liability agreements
- Investigate suspicious activities to reduce or eliminate Diebold Nixdorf's liability exposure
- Investigate employee theft and mismanagement of customer assets, work with authorities for prosecution, and assist and support law enforcement investigation requests

Security by Design

- Derive and implement security design principles into development processes and solutions
- Embed incident-related information into new product development
- Complete internal security assessments and penetration tests before product releases

Attack Categories

The cybersecurity industry has created three distinct categories for fraud and security incidents: data, physical and cyber. Each category has unique characteristics describing the methods by which a criminal may attempt to compromise a device using various levels of complexity.

Data Attacks

Aim to gain physical and/or digital access to card data

Skimming

Shimming

Software Skimming

Eavesdropping

Card Trapping

Physical Attacks

Seek access to ATM cash

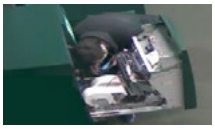
Explosion

ATM Burglary

Ram Raids

Internal Misuse

Cash Trapping

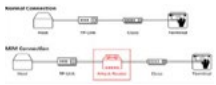


Preparation

Cyberattacks

Strive for physical and/or digital access to systems, communications, data and ATM cash

Jackpotting



Host Spoofing

Ransomware

Transaction Reversal Fraud

Denial of Service

Data Breach

Subscribe to the Global Security Portal

For more information and alerts about trending attacks, subscribe to our Global Security Portal. To access the site, follow the directions in the Global Security Portal section of this document on Page 20.

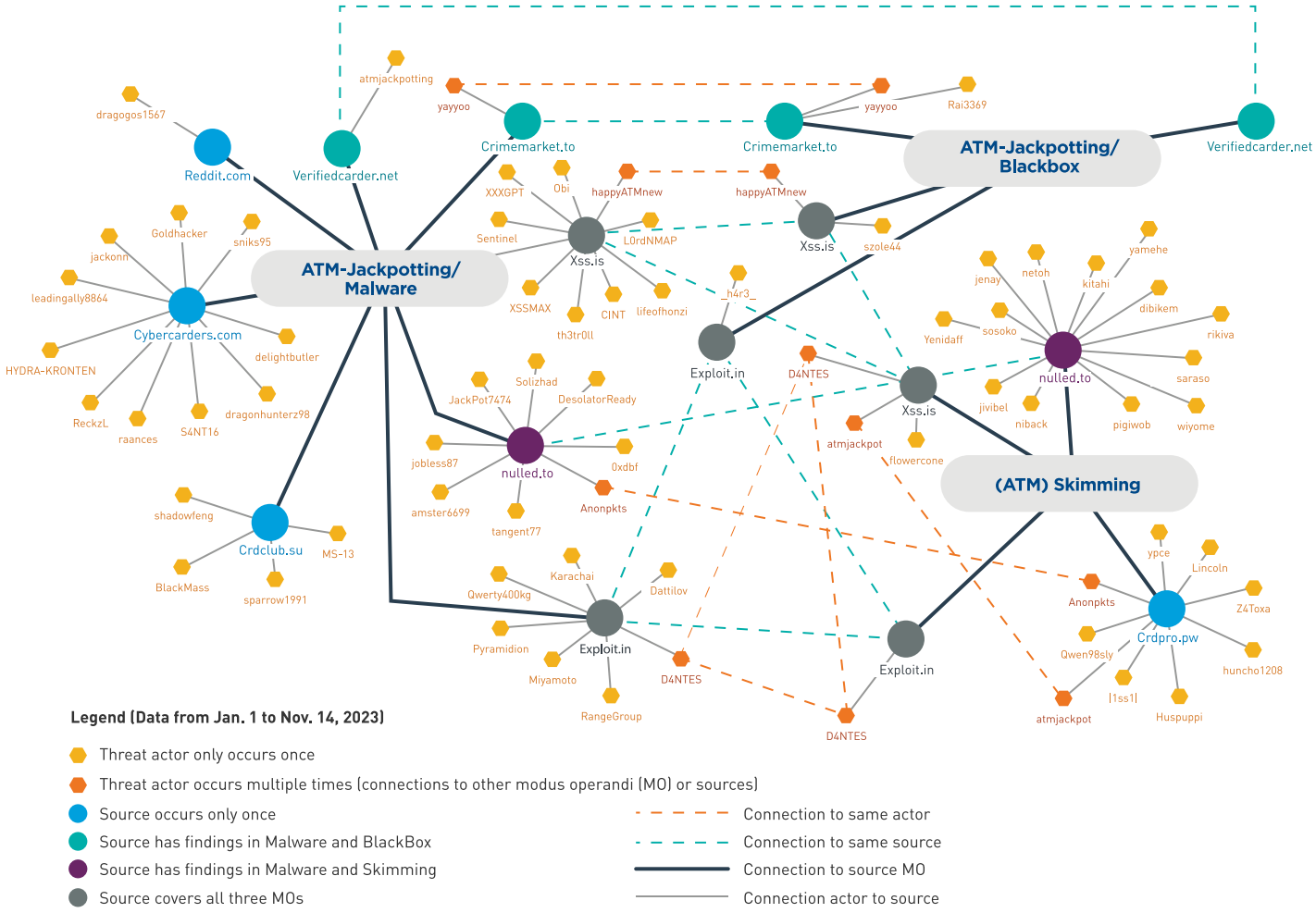
Overview of Threats Targeting the Banking Industry

As previously mentioned, Diebold Nixdorf is gathering open-source intelligence, in addition to deep web and darknet intelligence, with support from various services.

The essential tasks of collecting and evaluating information encompass a wide range of communication channels used by threat actors, including WhatsApp, Telegram, Reddit, closed forums/chat groups and the darknet.

We created the following diagram to offer a glimpse into the dynamic landscape of threats targeting the banking industry, specifically ATM hackers. It delineates various threat actors and the secure channels they employ to share knowledge, tools and techniques and discuss potential attacks. This constant exchange fuels their criminal enterprises and makes them formidable threats to financial institutions.

2023 Self-service Dark Ecosystems Snapshot: Interrelation of Actors, Attacks and Underground Markets



Legend (Data from Jan. 1 to Nov. 14, 2023)

- Threat actor only occurs once
- Threat actor occurs multiple times (connections to other modus operandi (MO) or sources)
- Source occurs only once
- Source has findings in Malware and BlackBox
- Source has findings in Malware and Skimming
- Source covers all three MOs
- Connection to same actor
- Connection to same source
- Connection to source MO
- Connection actor to source

Central players like ATM-Jackpotting/BlackBox orchestrate complex attacks, while others like Sentinel distribute malware to infiltrate ATM systems. Information brokers like D4NTES keep the network informed, while tangent77 and MS-13 provide logistical support. Many individuals and groups are connected by a shared goal: exploiting vulnerabilities in ATMs for financial gain.

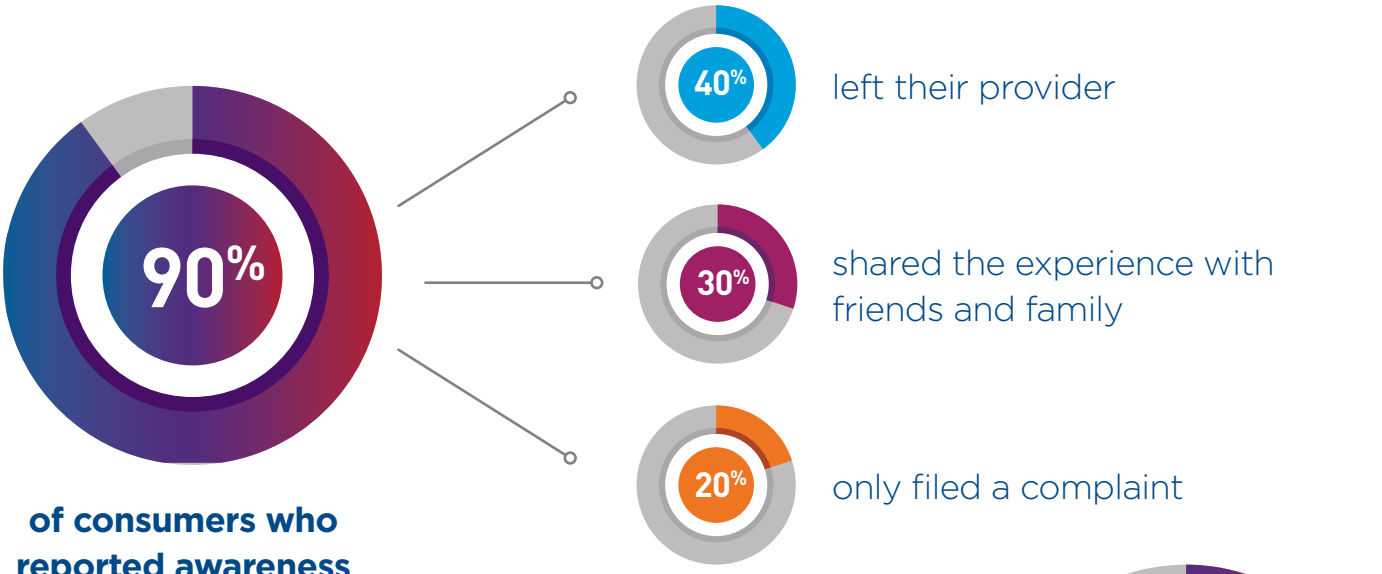
Aligning Customer Concerns with Information Technology Investments

Threat intelligence and cybersecurity are complex fields that require constant attention. Statistics show that consumers are also paying closer attention to current events and have increased concerns about the security of their banking experiences – and they will leave providers that are not secure. The best user experience will not matter if it's not trusted.

According to Aite-Novarica Group's Banking IT Budgets and Projects 2023 survey[1], banks self-rate their IT security capabilities the highest among all core systems. They believe ongoing investments and attention in this area should continue to pay off. These expenditures are essential because most institutions are experiencing increased attacks with dynamic, new patterns.

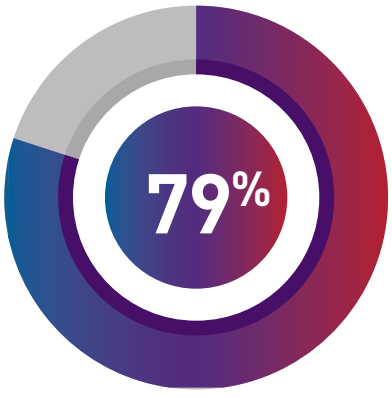
To maintain companies' levels of self-assurance – which translates into customer confidence – ongoing attention and investment are required. It is challenging to keep increasingly complex security infrastructures up-to-date, and attackers quickly spot and exploit weak spots in companies' defenses. That's why creating the modern, secure experiences consumers expect must be a never-ending process of assessing and improving.

Even so, less than half of the banks surveyed expect to increase their investments in IT security from 2023 through 2025[1].



of consumers who reported awareness of a security breach in digital banking at their primary provider took action

of financial institutions reported an increase in cyberattacks



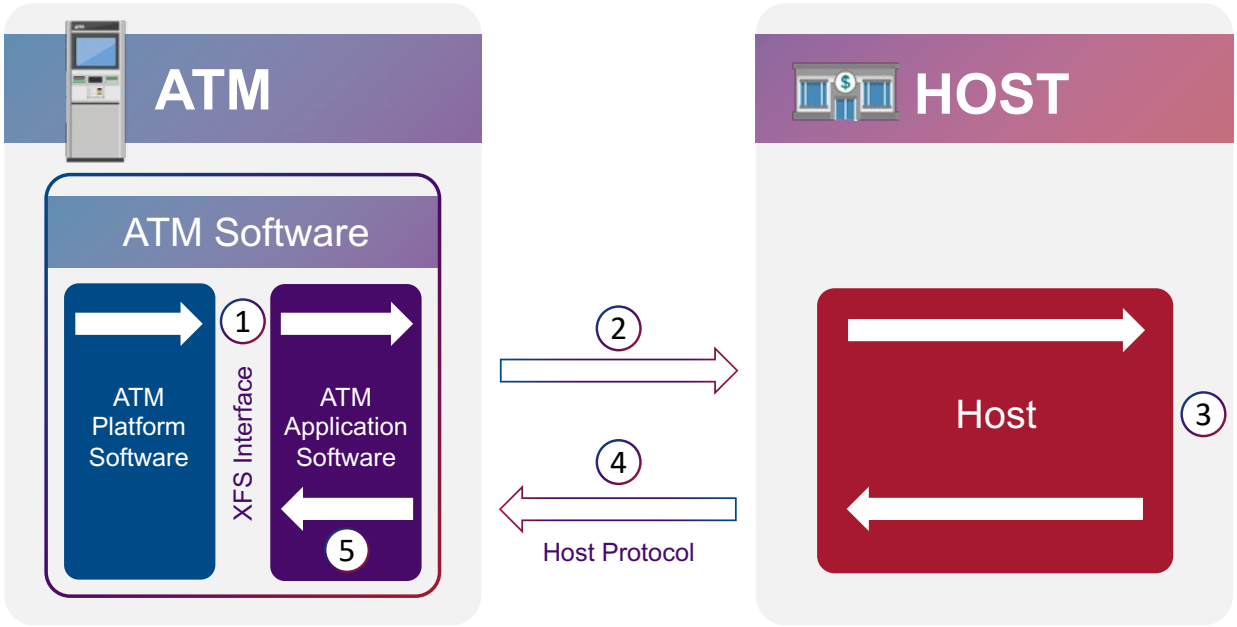
[1] Aite-Novarica Group. Banking IT Budgets and Projects 2023. Figure 17 – Core Investment Plans 2023.
Figure sources: NielsenIQ International Retail Banking Consumer and Technology Survey, commissioned by Diebold Nixdorf; http://purplesec.us/resources/cyber-security-statistics/#financial

Spotlight: Banking Host Spoofing

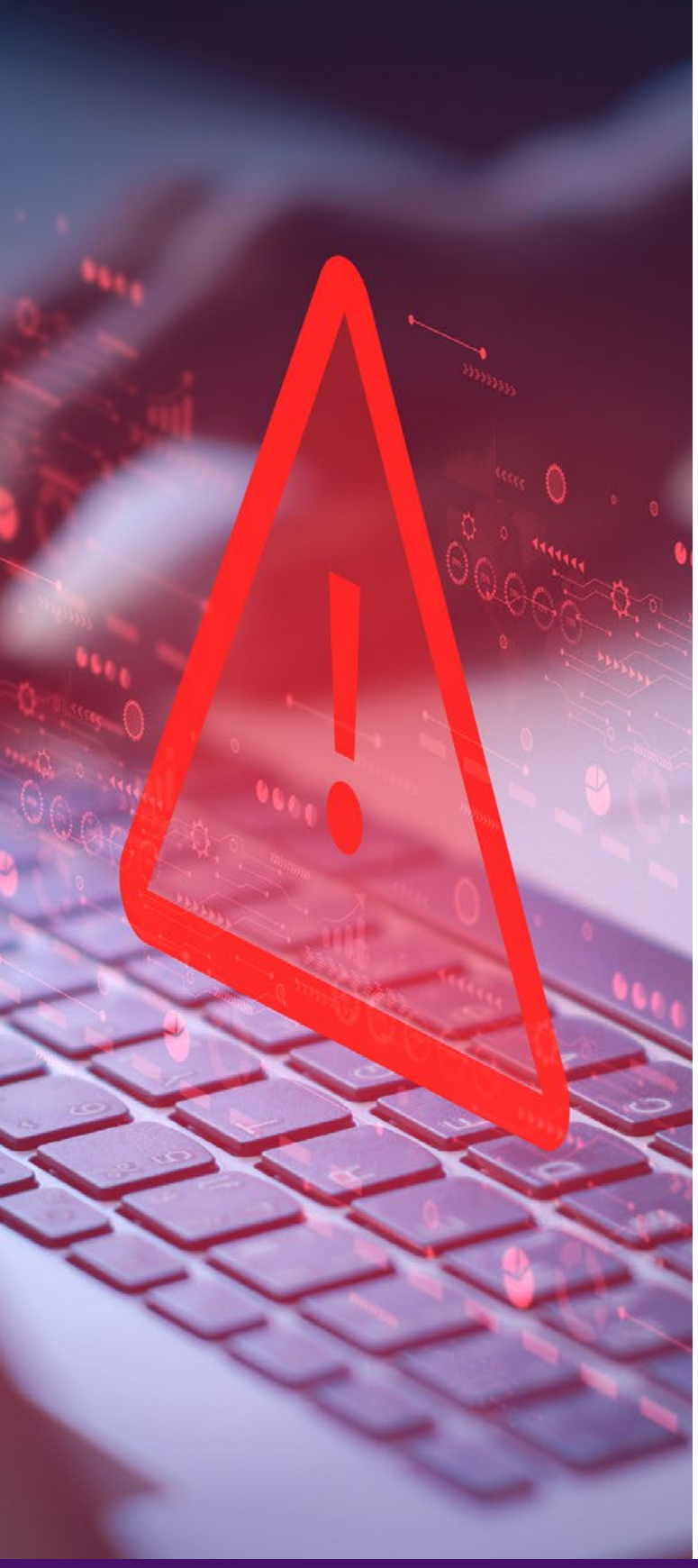
Cybercriminals frequently target the banking industry, which impacts financial institutions and their customers. On the one hand, attackers strive to get cash illegitimately out of the ATM. On the other hand, they steal information, acquire consumer debit/credit card data, clone card(s) and withdraw cash.

In modern banking environments, any withdrawal needs authorization from either the bank's central transaction server or a payment network the bank is linked to (e.g., FIS, Jack Henry). These authorization instances are generally referred to as "hosts." "Host spoofing" is manipulating the communication from the host's server to the ATM to help the attacker withdraw cash without debiting the customer's account.

Typical Communication Flow Between ATM and Bank



1. ATM assembles message to request withdrawal authorization from host
2. ATM sends message to host
3. Host process withdrawal request
4. Host tells ATM to dispense money or denies request
5. If approved, ATM dispenses cash



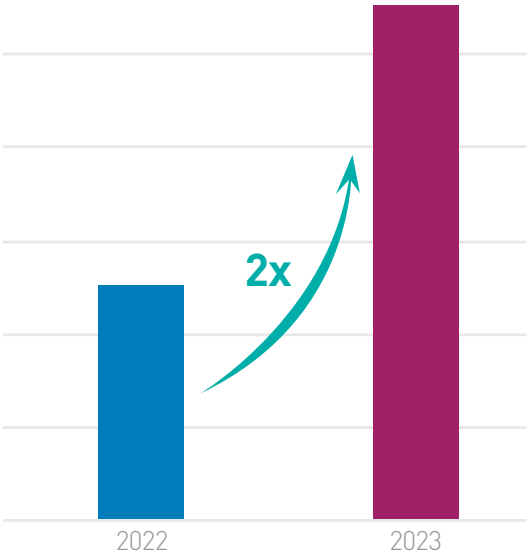
Description of the Attack

In a host spoofing attack, a criminal uses malware on a physical device connected to the network (similar to a router) to impersonate the host.

The host appears legitimate to the ATM and responds with valid messages based on the typical protocol. Host spoofing aims to send illegitimate dispense authorizations or modify the amount in legitimate host responses without notifying the host of the actual money that has been distributed.

Host spoofing attacks can be divided into two categories: man-in-the-middle and host replacement. Each requires different levels of access to the ATM or the infrastructure.

Reported Cybersecurity Attacks at Diebold Nixdorf



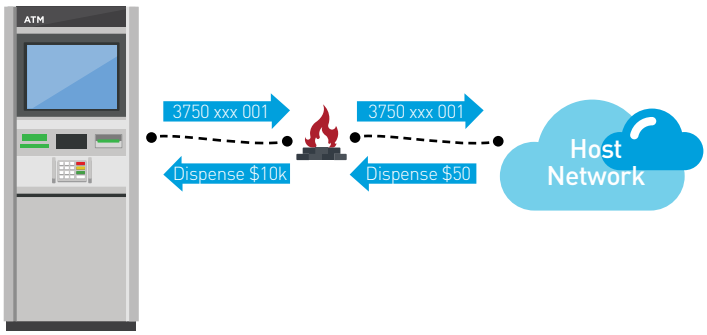
The total number of all reported attacks at Diebold Nixdorf more than doubled from 2022 to 2023. Customers in the United States reported the vast majority of the incidents. As the number of incidents increases, it's critical for customers to be aware of these attacks, how they are facilitated and the countermeasures that they can deploy.

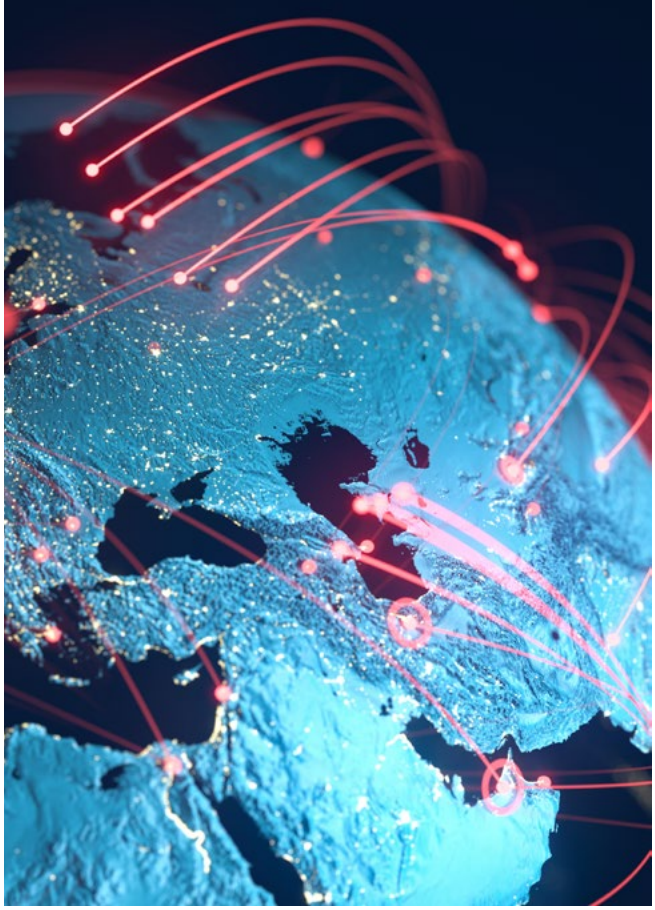
Learn More About Host Spoofing

For more information, review the Host Spoofing Fact Sheet on the Global Security Portal. To access the site, follow the directions in the Global Security Portal section of this document on Page 20.

Man-in-the-Middle

Man-in-the-middle attacks are one variant of host spoofing. After infiltrating the network communication, the malicious component listens to and alters transaction data exchanged between the ATM and the host. The goal of this type of host spoofing is data manipulation of the authentic dispense authorization messages to increase the amount of money distributed by the ATM.

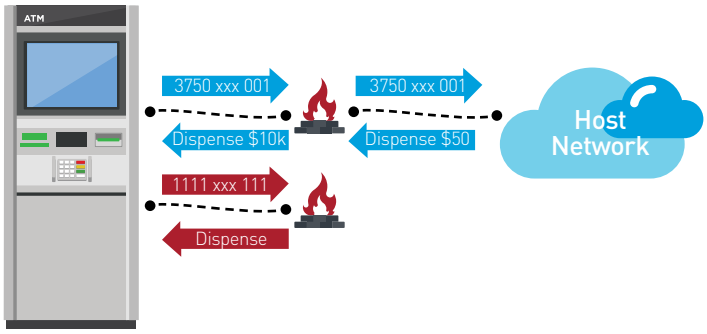




Host Replacement

The second variation of host spoofing is host replacement. The malicious component acts as a proxy that intercepts legitimate transaction requests and responds to the ATM appropriately to authorize cash withdrawals.

The replacement can be a complete substitution where the authentic host does not know any transactions are occurring. Alternatively, it may be a partial replacement, where the malicious component only intercepts requests involving certain card numbers without impairing other transactions. This specification allows the attacker to use predetermined, preprogrammed, invalid or fake debit/credit card(s) to dispense money.



Recommendations to Protect Against Host Spoofing

Since host spoofing targets network communications, both the ATM and its host must be logically secured using hard disk encryption and runtime integrity protections.

Additionally, network traffic between these endpoints should be protected with a message authentication code (MAC) and/or transport layer security (TLS) to authenticate and validate host messaging. Without these protections, transaction messages could be maliciously modified but interpreted by an ATM as legitimate responses from the host.

Current host spoofing trends show fraudsters specifically target terminals on networks configured to use default clear-text network communication because the ATM cannot validate the integrity or authenticity of host messaging. ATM network implementations should leverage the confidentiality, integrity and authenticity protections offered by MAC or TLS to deter these attacks. It is crucial to proactively validate and test your security configurations and implementations to protect terminals from being victims of these types of attacks.

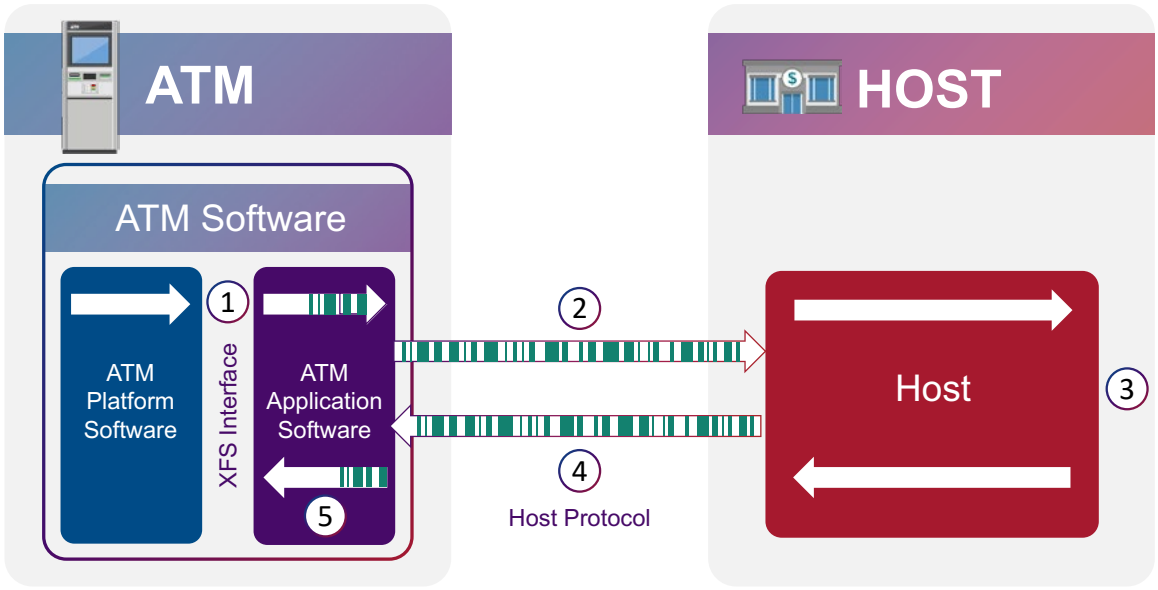
Message Authentication Code

A message authentication code (MAC) is a string of code that identifies who created or sent a message and if it has been modified. It provides a way to ensure that content transmitted between the ATM and the host is authentic and unaltered by host spoofing attacks.

MACing has been an essential part of major authorization protocols between ATMs and banks' hosts from the early days of ATMs. It is standardized and can be used to maintain message integrity at the application level by securing single, multiple or all elements of the authorizations, ensuring both security and performance. The selection of data elements to be secured may differ depending on the bank's needs.

It is highly recommended to require and validate the authenticity and integrity of all communications to and from the host by implementing MACing. This solution should include communications with the terminal and issuer of financial request-response messages.

Using Message Authentication Code Protections

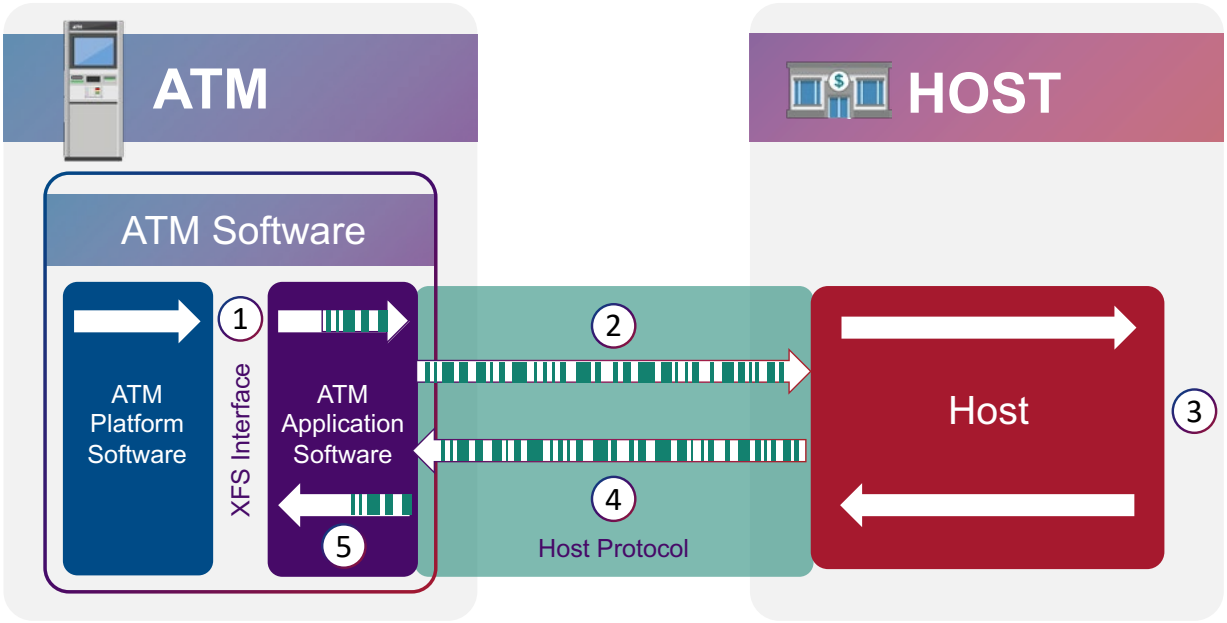


1. ATM assembles message to request withdrawal authorization from host
2. ATM sends message with *secured (aka "MAC"ed)* elements to host
3. Host process withdrawal request
4. Host tells ATM to dispense money or denies request *in a message with secured elements*
5. If approved, ATM dispenses cash

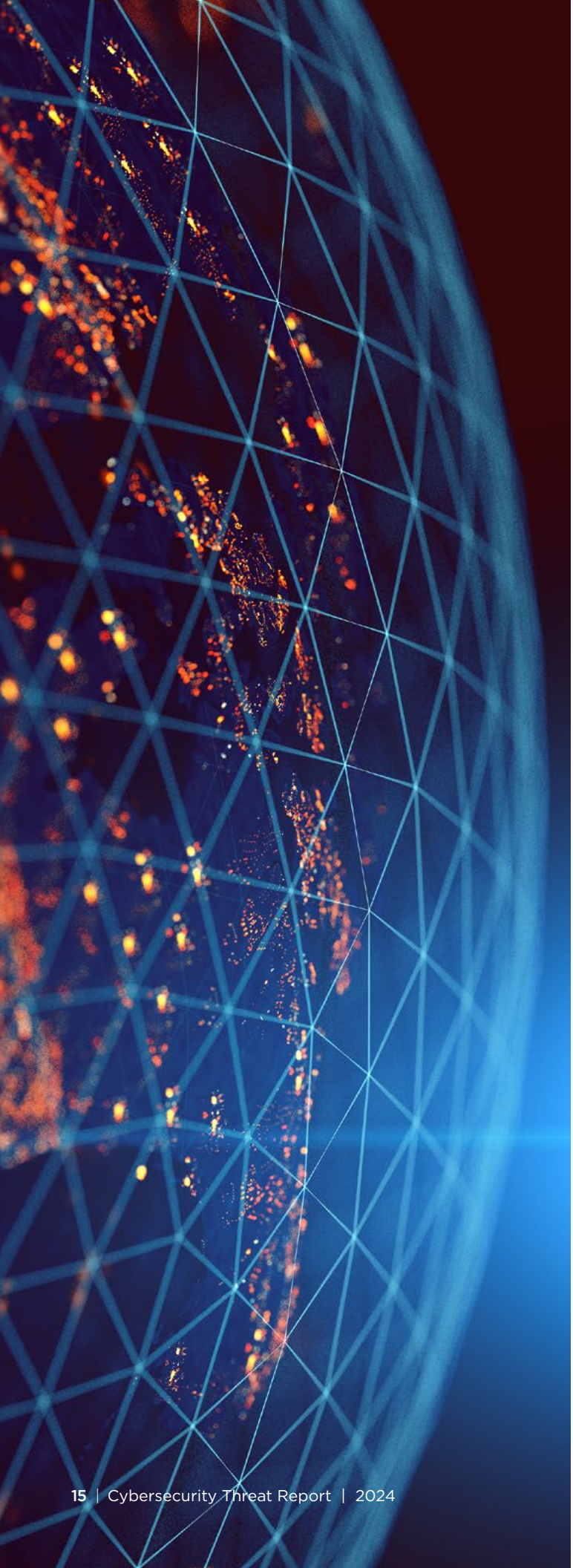
Transport Layer Security

Transport layer security (TLS) encrypts data to ensure that cybercriminals cannot see information that is being transmitted between the ATM and the bank's host. TLS must start within the ATM's application software to be the most effective. However, it might end at the host or the bank's data center. The most secure option would be a combination of both MAC and TLS.

Using Message Authentication Code Protections with Transport Layer Security



1. ATM assembles message to request withdrawal authorization from host
2. ATM sends message with secured (aka "MAC"ed) elements *wrapped in TLS* to host
3. Host process withdrawal request
4. Host tells ATM to dispense money or denies request in a message *secured by MAC and TLS*
5. If approved, ATM dispenses cash



Network Security

In the present landscape, a notable challenge in network security stems from the transformative shift toward open technologies. The conventional understanding of network security faces a dilemma as customers and manufacturers extend their operations beyond the confines of closed networks. The core issue lies in the potential vulnerabilities introduced by this shift, urging a reassessment of network segmentation strategies.

The Challenge

The evolving use of open technologies introduces a complexity that traditional network segmentation may struggle to address adequately. The risk of security breaches escalates as interactions extend beyond conventional boundaries. This shift challenges the effectiveness of existing segmentation practices, potentially exposing organizations to new forms of cyberthreats.

Best Practices

Adaptability to Open Technologies

A robust segmentation strategy should be agile enough to accommodate the integration of open technologies without compromising security.

Ensuring Interaction Integrity

The focus should be on securing web services and APIs to maintain the integrity of interactions that extend beyond traditional boundaries.

Seamless Incorporation of External Elements

Network segmentation should seamlessly integrate open and private cloud environments, fostering a cohesive and secure operational environment.

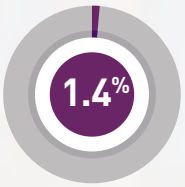
Spotlight: Retail Shrink

Unintentional errors during transactions, consumer and/or employee theft (called "sweethearting"), and other thefts are also known as shrink. They are all significant problems in retail and directly correlate with profit. Most shrink occurs during the sales process rather than by targeting devices such as self-checkouts (SCOs) and electronic points of sale (EPOS). Unfortunately, consumers and employees may be involved in these scenarios.

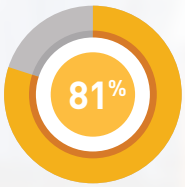
The increase in incidents and new types of theft are encouraging retailers to invest in new technology – including the latest developments in artificial intelligence (AI). Several solutions can help detect exactly where shrink is occurring and can be customized based on the retailer's specific needs.

Shrink: By the Numbers

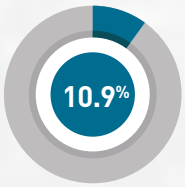
of inventory shrink can be attributed to theft.



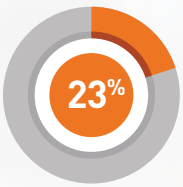
average shrink as a percentage of total retail sales[1]



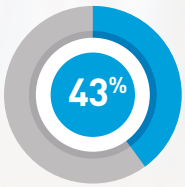
retailers that reported an increase in shrink in 2022[2]



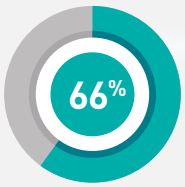
theft losses that are recovered, which translates to $8.18 lost for every $1 recovered[1]



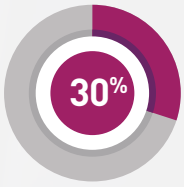
estimated that unmonitored self-checkout systems accounted for as much as 23% of their total unknown store losses[3]



of self-service losses are caused by malicious behavior[3]



think that the problem of SCO-related losses was becoming more of a problem in their businesses[3]



increase in losses of retail sales[3]

[1] National Retail Federation. National Retail Security Survey 2022

[2] Jack L. Hayes International. Annual Retail Theft Survey 2023

[3] Global Study on Self-Checkout in Retail, ECR Retail Loss Group, 2022

Retail Shrink: A Threat Intelligence Perspective

Within the complex retail landscape, the challenge of shrink emerges as a pivotal focus of threat intelligence. Unlike traditional approaches that target devices like SCOs or EPOS, most shrink occurs during the sales process, directly impacting inventory. In 2023, our threat intelligence team examined diverse sources such as 4chan, Twitter, Sinister, Discord and Pastebin, unearthing discussions that shed light on the alarming rise of retail shrink.

Threat actors proudly share their exploits, boasting about successful endeavors at various retailers. Their unsettling sentiments, such as "I regularly steal from Retailer X; they can afford it." underscore their audacious nature, necessitating a robust response from the retail industry and its partners.

Diebold Nixdorf's commitment to threat intelligence goes beyond being a technology provider. We serve as trusted experts to help others navigate the ever-evolving landscape. By dissecting and interpreting threat actor discussions, we equip retailers with the knowledge to not only detect and prevent shrink but also stay one step ahead of adversaries. As we explore the intersection of technology and threat intelligence, we aim to empower retailers with actionable strategies and a comprehensive understanding of the challenges they face in safeguarding their assets.

Analyzing Shrink in Stores

Based on extensive in-store analysis and monitoring of customer behavior around SCOs, Diebold Nixdorf created a list of use cases for retail transactions that helped us understand how and when shrink occurs. Further testing and observation led us to an extensive list of the most frequent actions that lead to shrink. These actions can be categorized into three types: missed scan, walk away or barcode switch. These categories and actions help us share insights with our partners and create solution requirements for our products to mitigate shrinkage across the retail industry.

Missed Scan

- Intentional non-scan (theft)
- Unintentional non-scan (error)
- Multipack (scan only one item of several)
- Item left in hand or basket
- Item in output area at start of transaction

Walk-Away

- Incomplete transaction (scan but no pay)
- Partial payment of transaction
- No transaction (no scan, no pay -> walkout)

Barcode Switch

- Item switching
- Product stacking
- False barcode
- Loose items labels

Using Computer Vision with AI to Prevent Loss at Self-Checkouts

AI-driven shrink-reduction solutions can detect products on shelves or in bags, baskets and carts and track them as the shopper moves the items to the bagging area. The shopper's actions – picking up products, passing them across the scanner or not, placing them in another location – are also monitored. Due to the possible deep integrations of these solutions with SCO software, they can determine if an item was scanned as expected or if a scan was incomplete.

Diebold Nixdorf has integrated these advancements into our SCO offerings to combat shrink. Computer vision uses machine learning (ML) and deep learning models to identify and classify objects in videos and images. Based on ML, our computer vision monitors every transaction at the SCO, in the checkout area and within its AI. Advanced SCOs equipped with security scales and USB and internet protocol (IP) cameras can provide a stream of inputs to the computer vision and AI models, which watch for unintentional mistakes and intentional shrink. Thanks to the flexible and unique notification system, which includes shopper nudges to do the right thing, staff alerts or SCO blocks, retailers secure their revenue and store employees can focus on supporting customers.

Actions Detected by Computer Vision with Artificial Intelligence

- **Item in bag** at transaction start "own bag" selected
- **Barcode switch** with fresh produce item weighed and coded elsewhere
- **Item switch** with similar weight, e.g., expensive wine for cheap
- **Missed Scans**: items left in basket, e.g., multipacks; item on security scale at transaction start

Threat Intelligence Best Practices for the Industry

Data Analytics and Pattern Recognition

Harnessing the power of data analytics and pattern recognition is instrumental in identifying anomalies that could signify potential theft. Analyzing transaction patterns, inventory data and employee behavior allows retailers to detect irregularities and take preemptive action before losses escalate.

Employee Training and Awareness

Employees play a crucial role in preventing shrinkage. Comprehensive training programs that educate staff about theft indicators, security protocols and the importance of vigilance contribute significantly to creating a united front against theft. Fostering a culture of awareness and accountability among employees strengthens the overall security posture.

Collaborative Information Sharing

Engaging in collaborative information sharing among the retail industry and law enforcement agencies enhances the collective ability to combat shrink. Establishing networks to share threat intelligence, best practices and emerging trends enables retailers to stay ahead of evolving tactics employed by threat actors.

AI Solutions

Embracing AI solutions, particularly computer vision, empowers retailers to proactively identify suspicious activities at various touchpoints, such as self-checkouts. AI-driven systems can analyze behaviors, recognize theft-related patterns and trigger real-time alerts for immediate intervention.

Auditing and Regular Assessments

Regular audits and assessments of security protocols, inventory systems and surveillance infrastructure are essential. These proactive measures identify vulnerabilities, ensure the effectiveness of implemented strategies and provide insights for continuous improvement.

Global Security Portal

Diebold Nixdorf remains dedicated to proactive communication and collaboration, empowering you to stay ahead of evolving security threats. We offer our partners exclusive access to our advanced Global Security Portal, a centralized hub for comprehensive threat intelligence, enabling you to respond swiftly to fraud and gain insights into emerging trends and threat actors.

In the portal, you can review the detailed security incident map that tracks current activity, choose from a range of communication options to stay informed about existing and emerging trends, and learn how to take early measures to safeguard your operations. You can also learn about the **Analyze, Communicate and Track (ACT)** methodology, which is at the core of our global security strategy. It provides a dynamic framework for addressing security threats worldwide and is integrated into the site, including:

1. **ACTive Security Alerts:** Receive real-time alerts to stay informed about imminent threats
2. **fACT Sheets:** Access in-depth resources providing actionable insights into specific threat scenarios
3. **ACTive Security Notifications:** Stay updated on the latest security developments with timely notifications
4. **Attack Type Definitions:** Understand the nature of various cyberthreats and their implications

Our Frequently Asked Questions section also serves as a valuable resource, addressing queries relevant to all users of the Global Security Portal. It is the primary point of contact for inquiries about the service and website.

Sign Up for the Global Security Portal Today

To access the portal and receive ACTive security alerts, register at:
https://www.dieboldnixdorf.com/en-us/support/globalsecurityportal/subscribe/

More Secure: 7 Shields to Protect the Self-service Channel

Security at the self-service channel is critical: cash, customer data and financial transactions need to be protected from all sides.

By taking a comprehensive look at the entire ecosystem, our security specialists identified seven shields to secure ATM fleets long-term. For more information, get the Make Your ATM Network More Secure guide on DieboldNixdorf.com.

Security Assessments

Attack patterns and security technology change and develop quickly. To ensure your self-service channel continues to be secure, conduct regular security assessments to expose weak points.

Physical Security

Using brute force to get to the cash inside the ATM continues to be the weapon of choice for some attackers. There are several measures you can take to protect against this.

Data Security

Some steal the card data and PIN of consumers, so they can then access their victims' accounts. You can prevent this by ensuring the privacy of users and using a secure card reader.

Security Monitoring

A quick reaction to an attack can make a decisive difference. The easiest way to ensure this is to closely monitor the self-service fleet to detect possible fraudulent activity in real time.

Process, Procedures & Compliance

Secure and compliant procedures should be implemented throughout an ATM's lifecycle: the development process, the installation and the day-to-day operation.

Cooperation & Collaboration

Information sharing among all players — financial institutions, law enforcement and ATM manufacturers, and software and service providers — is key to quickly analyze and counteract new security threats.

Cybersecurity

Cyberattacks have become more common. Securing the communication between components of the ATM and the host as well as preventing unauthorized access to devices and information are effective countermeasures.

Conclusion: Elevating Security Through Threat Intelligence Mastery

By exploring cybersecurity intricacies within the banking and retail industries, this report provides insights for safeguarding against contemporary threats. It addresses the delicate balance between technological innovation and escalating risks, emphasizing the crucial role of threat intelligence as a proactive and transformative force.

Key Insights

1. **Proactive Defense for Future Assurance:** Taking a proactive approach to anticipating and counteracting threats is essential. In the world of threat intelligence, knowledge becomes foresight, empowering organizations to thwart adversarial moves in advance and safeguard their organizations.

2. **Collaboration:** Just as Diebold Nixdorf builds and maintains alliances with industry leaders, your organization must also build a network of reliable information. Our approach highlights how information exchange can be a force multiplier, countering the growing sophistication and specialization of cyberthreats.

3. **Global Security Portal:** At the core of this transformative approach is the Global Security Portal, positioned as more than a reactive tool. It serves as a beacon of insight, providing subscribers with alerts and a deep understanding of emerging trends. This type of nuanced comprehension enables organizations to strategically fortify their defenses against the ever-evolving threat landscape.

Acknowledgments

We extend our gratitude to the dedicated contributors, researchers and professionals who generously shared their expertise in creating this report. Their commitment to the security and resilience of the banking and retail industries is evident, and their insights contribute significantly to our collective journey toward a more secure digital future.

Diebold Nixdorf