CENTRAL BANK OF EGYPT
Egyptian Banking Institute

البنك المركزى المصرى
المعهد المصرفى المصرى

June 2023

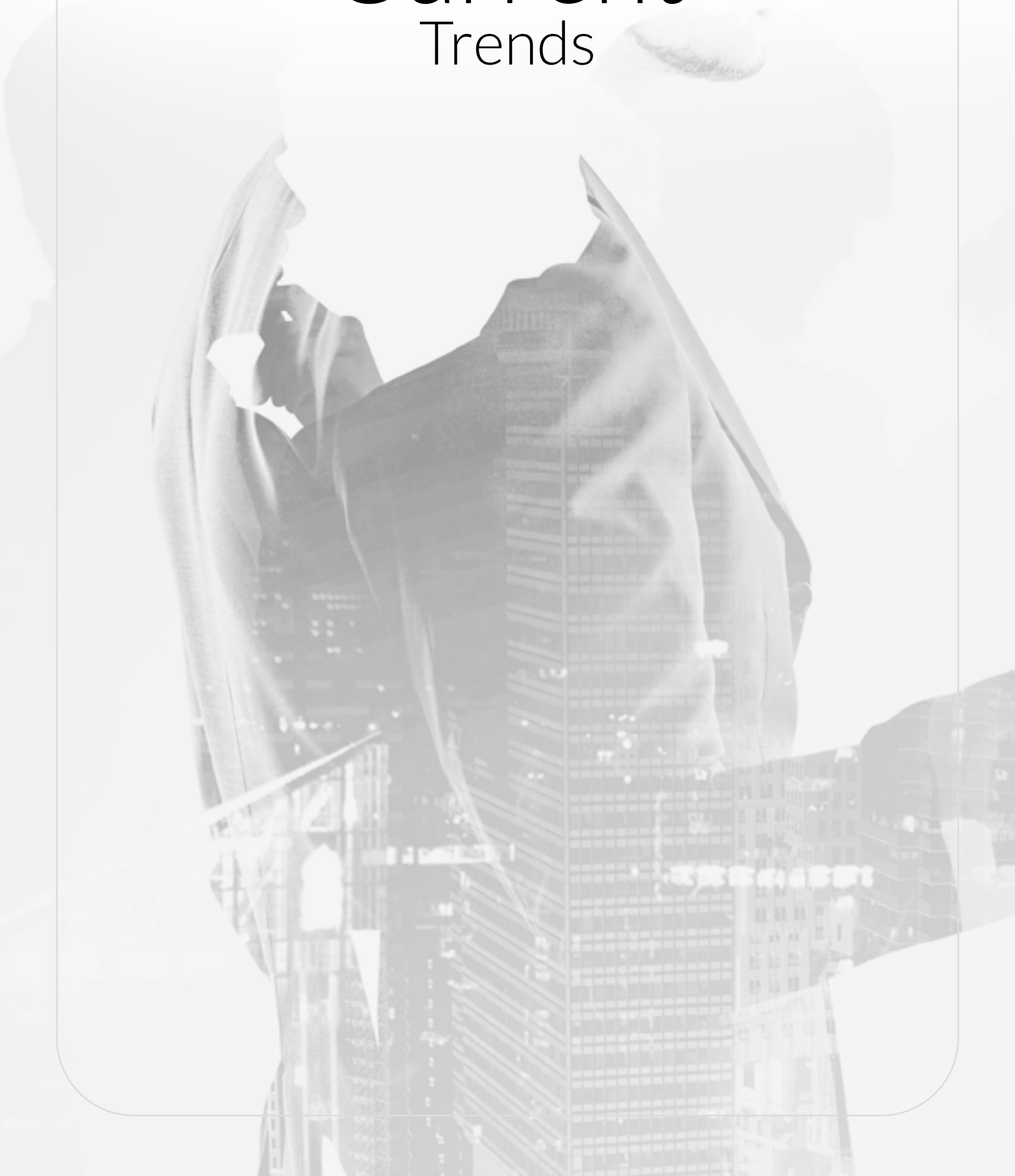
Current Trends

"Zero Trust Policy in the Banking Sector"

www.ebi.gov.eg

June 2023

Current Trends



Background

Legacy perimeter-based defense models used by financial institutions (FI) are insufficient to prevent malicious actors from causing financial, operational, reputational and client harm. The annual Verizon Cybersecurity Report shows that individuals are the weak link in security – whether clicking on malware or otherwise being socially engineered to provide credentials.

This allows malicious actors to obtain access to the network, perform reconnaissance, identify high-value assets and move laterally within the organization to achieve their intent. Zero Trust is an approach that seeks to mitigate the risks associated with this scenario. It assumes that a malicious actor is already within an FI's network and uses a variety of strategies to reduce the likelihood that the threat actor (or careless insider) will move laterally through the network or elevate their privileges.

Concept and Definition

Zero Trust is a security framework and policy approach that has gained significant traction in the banking sector and other industries. It is designed to enhance the security posture of organizations by assuming that no user or device should be automatically trusted, regardless of their location or network privileges. Instead, Zero Trust requires continuous verification and authentication of all users, devices, and applications attempting to access sensitive resources.

In the banking sector, where protecting customer financial data and preventing unauthorized access to critical systems are paramount, Zero Trust policies are crucial.

Here are some key aspects of Zero Trust policies:

1. **Principle of Least Privilege:** Zero Trust is based on the principle of least privilege, which means granting users only the minimum level of access necessary to perform their specific tasks. This approach reduces the risk of unauthorized access to sensitive financial data and limits the potential damage if a user's account is compromised.
2. **Network Segmentation:** Zero Trust encourages network segmentation to create micro-perimeters within an organization's infrastructure. By dividing networks into smaller, isolated segments, the potential impact of a security breach or lateral movement of attackers is limited.
3. **Identity and Access Management (IAM):** Zero Trust emphasizes robust identity and access management practices. This includes multi-factor authentication (MFA), strong password policies, and continuous monitoring of

user behavior and privileges. IAM systems help ensure that only authorized individuals can access sensitive systems and data.

4. **Continuous Monitoring and Analytics:** Zero Trust requires continuous monitoring and analysis of user behavior, network traffic, and application activity. This helps identify anomalies, potential security threats, and suspicious activities, allowing for timely detection and response to security incidents.
5. **Secure Access Technologies:** Implementing secure access technologies, such as virtual private networks (VPNs), firewalls, and secure web gateways, is essential in Zero Trust. These technologies help enforce policies and provide additional layers of security for remote access and external connections.
6. **Application-Centric Security:** Zero Trust focuses on securing individual applications rather than relying solely on network perimeter defenses. Each application is treated as an independent entity, and access is granted based on user identity, device security posture, and contextual information.
7. **Automation and Orchestration:** Zero Trust policies are often supported by automation and orchestration tools. These tools help streamline security operations, enforce consistent policy enforcement, and facilitate real-time threat response.

Importance

The importance of implementing a Zero Trust policy in the banking sector cannot be overstated. Here are some key reasons why Zero Trust is crucial in banking:

1. **Protection of Customer Data:** Banks handle vast amounts of sensitive customer data, including financial information, personal identification details, and transaction records. Implementing a Zero Trust policy ensures that access to this data is highly controlled, minimizing the risk of data breaches and unauthorized access.
2. **Mitigation of Insider Threats:** The banking sector faces the risk of insider threats, where authorized individuals with legitimate access may misuse their privileges or become compromised. Zero Trust principles, such as the principle of least privilege and continuous monitoring, help identify suspicious behavior and limit the potential damage caused by insider threats.
3. **Prevention of Lateral Movement:** In a traditional network setup, once an attacker gains access to a system, they can move laterally across the network, potentially accessing other sensitive resources. Zero Trust's network

segmentation and micro-perimeter approach limit an attacker's ability to move laterally, containing the impact of a security breach and reducing the attacker's ability to escalate privileges.

4. **Protection against External Attacks:** Zero Trust policies reduce the attack surface by requiring constant verification and authentication of users, devices, and applications. This helps protect against external attacks, including phishing attempts, malware infections, and unauthorized access attempts.
5. **Compliance with Regulatory Requirements:** The banking sector is subject to strict regulatory requirements regarding data security and customer privacy, such as the Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation (GDPR). Implementing a Zero Trust policy can assist banks in meeting these compliance obligations by enforcing strong access controls and monitoring mechanisms.
6. **Enhanced Remote Work and Mobile Security:** With the rise of remote work and the increasing use of mobile devices, banks need to ensure secure access to critical systems and data from any location. Zero Trust policies provide a framework for secure remote access, requiring authentication and verification regardless of the user's location or network connection.
7. **Proactive Threat Detection and Response:** Zero Trust emphasizes continuous monitoring, behavioral analytics, and threat intelligence integration. This enables banks to identify potential security incidents in real-time, respond promptly to emerging threats, and prevent or minimize the impact of cyber-attacks.

By implementing a Zero Trust policy, banks can significantly strengthen their security posture, protect customer data, mitigate the risk of insider and external threats, and ensure compliance with regulatory requirements. It establishes a proactive and layered security approach that is well-suited to the evolving threat landscape in the banking sector.

Practices in the banking sector

Several banks have embraced the Zero Trust policy and implemented related practices to enhance their security posture. While specific details may vary, here are a few examples of banks that have applied Zero Trust principles:

1. JPMorgan Chase: JPMorgan Chase, one of the largest banks globally, has adopted a Zero Trust approach to enhance its security measures. They have implemented strong access controls, including multi-factor authentication and strict identity verification processes. They also utilize continuous monitoring and behavior analytics to detect anomalies and potential threats.
2. Goldman Sachs: Goldman Sachs, a leading investment banking and financial services firm, has embraced Zero Trust principles to secure their systems and protect sensitive financial data. They have implemented network segmentation to isolate critical systems and implemented robust access controls, including least privilege and just-in-time provisioning. They also focus on monitoring user behavior and application activity to detect any suspicious activity promptly.
3. Citigroup: Citigroup has implemented Zero Trust practices to bolster its cybersecurity measures. They have adopted a Zero Trust architecture, securing individual applications and enforcing strict access controls based on user identities and device security posture. Citigroup also emphasizes continuous monitoring and threat intelligence integration to identify and respond to potential security incidents.
4. Barclays: Barclays, a multinational investment bank and financial services company, has incorporated Zero Trust principles into its security strategy. They have implemented strong identity and access management practices, including multi-factor authentication and role-based access controls. Barclays also leverages behavioral analytics and threat intelligence feeds to detect and mitigate potential threats in real-time.
5. Bank of America: Bank of America has been actively implementing Zero Trust principles to strengthen its security framework. They have embraced a Zero Trust architecture, focusing on secure access controls, identity verification, and continuous monitoring. Bank of America also emphasizes network segmentation and behavior analytics to mitigate the risk of unauthorized access and insider threats.
6. Wells Fargo: Wells Fargo has been investing in Zero Trust initiatives to bolster its cybersecurity defenses. They have adopted a Zero Trust framework that includes robust authentication mechanisms, continuous monitoring, and advanced threat intelligence. Wells Fargo prioritizes

granular access controls, limiting user privileges to reduce the risk of data breaches and unauthorized activities.

7. HSBC: HSBC, a multinational banking and financial services organization, has incorporated Zero Trust practices into its security strategy. They have implemented strong identity and access management controls, including multi-factor authentication and privileged access management. HSBC also utilizes behavioral analytics and anomaly detection to identify and respond to potential security threats promptly.
8. Standard Chartered: Standard Chartered has been adopting a Zero Trust approach to secure its systems and protect customer data. They focus on implementing strict access controls, network segmentation, and continuous monitoring. Standard Chartered also emphasizes the use of advanced analytics and threat intelligence to proactively detect and mitigate potential security incidents.
9. Deutsche Bank: Deutsche Bank has recognized the importance of Zero Trust in strengthening its security posture. They have implemented strict identity verification processes, including multi-factor authentication and continuous monitoring of user behavior. Deutsche Bank also emphasizes network segmentation and secure access controls to protect critical systems and data from unauthorized access.

These are just a few examples of banks that have embraced the Zero Trust policy and implemented related practices to enhance their security posture. Many other banks and financial institutions are recognizing the value of Zero Trust and actively adopting its principles to safeguard their systems, data, and customer information.

June 2023

Current Trends

HOTLINE
15200
One number to better serve you!

Headquarters – Nasr City
22 A, Dr. Anwar El Mofty St., Tiba 2000
P.O.Box: 8164 Nasr City, Cairo, Egypt

www.ebi.gov.eg

Like us on
facebook.com/EgyptianBankingInstitute

Follow us on
twitter.com/EBItweets

Join us on
linkedin.com/company/egyptian-banking-institute

Watch us on
YouTube Channel: Egyptian Banking Institute (EBI)