Strengthening Security for Banks and Customers

Authentication and Cybersecurity Best Practices

Who am I?

- Certified Information Security Manager - CISM
- Nearly a decade of experience in cybersecurity leadership, compliance, and defensive and offensive security
- Experienced vCISO
  - Building and managing cybersecurity programs
  - Managing compliance requirements
  - Managing cybersecurity incidents

The Cybersecurity Landscape

The Evolving Threat Landscape

- Verizon's Data Breach Investigation Report (DBIR) places the Finance Industry in:
  - 2nd / 21 in Incidents
  - 4th / 21 in Breaches
- Other Notables:
  - System Intrusion has overtaken Miscellaneous Errors and Basic Web Application Attacks as the primary threat in Financial and Insurance in 2024 indicating a shift toward more complex attacks.
  - System Intrusion, Miscellaneous Errors, and Social Engineering represent 78% of breaches.
- Cyberattacks are more advanced than ever:
  - Artificial Intelligence – automation and harder to detect
  - Phishing and Social Engineering – attacks are becoming increasingly targeted and convincing
  - Ransomware – higher ransoms and more sophisticated encryption

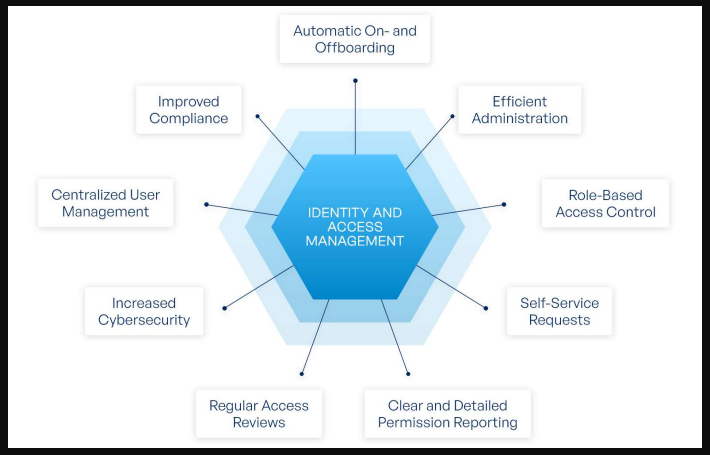
Consequences of a Data Breach

- Financial Loss:
  - Direct loss from theft
  - Recovery cost
  - Potential lawsuits
  - Cyber insurance premium increase
- Reputational Damage – Loss of customer trust and negative media coverage.
- Regulatory Fines – Non-compliance with regulations can lead to hefty penalties.
- Operational Disruption – Attacks can disrupt critical banking operations, impacting customers and business continuity.

Authentication

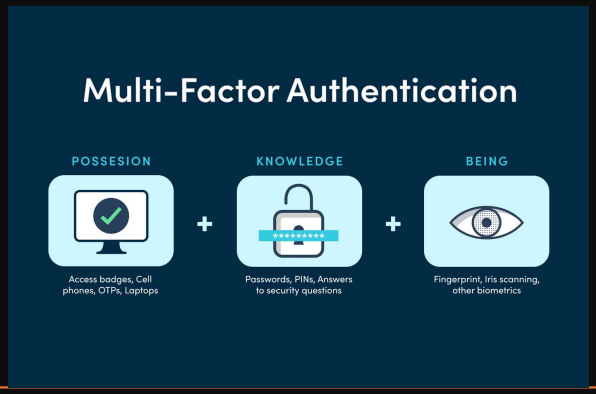
Identity and Access Management (IAM)

- IAM is a framework for managing digital identities and access privileges.
- Centralized system for managing users, roles, and permissions.
- Ensures that only authorized individuals can access sensitive data and systems.
- Streamlines user onboarding and offboarding process.



Adding Layers of Protection

- Multi-factor authentication requires users to provide multiple forms of authentication to verify their identity. At least two of the following:
  - Something you know (passwords, PINs, security questions)
  - Something you have (security tokens, authenticator apps, SMS codes, hardware keys)
  - Something you are (biometrics – fingerprint, facial recognition, voice recognition)
- Adaptive Authentication – Risk-based authentication that adjusts the required factors based on the user's context (location, device, behavior).



Password Management

- Passwords provide the ‘something you know’ aspect of multi-factor authentication.
- Create strong passwords that are difficult to crack.
  - Remember - ThatPasswordLength > C0mpl3x1ty
- Don’t use the same passwords for personal and business use.
- New NIST guidelines recommend not requiring password changes unless there is reason to (account compromise alerts, notifications of user credentials leaked on the dark web).
  - This increases the likelihood of a user creating a more secure password.
- Follow regulatory and compliance requirements! (Gramm-Leach-Billey Act (GLBA), NCUA, FFIEC, Cyber Insurance, etc.)

General Cybersecurity Best Practices

Security Awareness Training

- 88% of cybersecurity breaches are caused by human error (KnowBe4 / Stanford Research)
- Top reasons for clicking on phishing emails:
  - 43% perceived legitimacy (41% appears to come from a senior executive, 40% well-known brand)
- It is important to train your employees and customers on cybersecurity threats and how to recognize phishing scams and social engineering tactics.

Data Encryption

- Encryption transforms data into an unreadable format, making it useless to attackers even if they gain access (but don’t have the key).
- Essential for protecting sensitive financial information, customer data, and intellectual property.
- Used to secure data in both transit (e.g. during online transactions) and at rest (e.g. stored on laptops, desktops, servers).

Network Security

- Network security encompasses measures to protect the integrity and availability of computer networks and data.
- Prevents unauthorized access, misuse, modification, or denial of network resources.
- Examples of Network Security tools:
  - Firewalls, SIEM (Security Incident and Event Manager), logging, port security, and secure Wi-Fi
- Regular security assessments, patching, and vulnerability management, while boring to talk about, are the key to ensuring your environment is as secure as possible.

Device Security

- Device security focuses on protecting the endpoints (devices) that connect to the network.
- These devices can be vulnerable to malware, phishing attacks, and other threats.
- Strong device security is essential for preventing unauthorized access and data breaches.
- Examples of Device Security Tools:
  - Anti-Virus, Anti-Malware, EDR (Endpoint Detection and Response), Mobile Device Management (MDM)
- Software updates and antivirus software

Incident Response and Recovery

Incident Response Plan

- “It is not a matter of *IF,* but a matter of *WHEN*.
  - This saying has shifted to ‘not a matter of *WHEN,* but a matter of *HOW OFTEN*.’
- An Incident Response Plan is essentially the steps you will take in case of a cybersecurity incident.
  - Communication protocols and escalation procedures
- Minimizes damage and downtime.
- Swift and effective recovery is essential for restoring operations and maintaining customer trust.

Cybersecurity Insurance

- Cybersecurity insurance can help cover the costs associated with data breaches and other cyber incidents.
- Policies can cover legal fees, customer notification costs, data recovery expenses, and business interruption losses.
- Evaluate insurance options and choose coverage that aligns with the bank's risk profile.
- Know the requirements that are in the contract. If you don't follow the requirements, you may be denied coverage.

Questions