finovifi

CYBERSECURITY 101: PROTECTING YOUR ORGANIZATION IN THE DIGITAL AGE

COY OGLE

www.finovifi.com

OBJECTIVE

Provide a foundational understanding of cybersecurity tailored for banking professionals.

Key Message: Cybersecurity is critical to safeguarding sensitive financial data, maintaining customer trust, and ensuring compliance with regulations.

Why It Matters for Banks:

- Banks are prime targets for cyberattacks due to the high value of financial data.
- Regulatory requirements (e.g., GLBA, FFIEC, GDPR) mandate robust security measures.
- Breaches can lead to financial loss, reputational damage, and legal consequences.

Protect Data

Enhance Reputation

finovifi

COMMON CYBER THREATS FACING BANKS

> Phishing (Smishing)

- Fraudulent emails or texts tricking users into revealing credentials or downloading malware.
- Example: An email mimicking a bank's login page to steal employee or customer credentials.

> Ransomware

- Malware that encrypts data, demanding payment for decryption.
- Example: WannaCry attack impacted financial institutions globally.

> Data Breaches

- Unauthorized access to sensitive data (e.g., customer PII, account details).
- Example: Equifax breach exposed millions of records.

> Insider Threats

- Employees or contractors misusing access to steal data or disrupt operations.

> DDoS (Distributed Denial of Service)

- Overwhelming bank systems with traffic to disrupt online services.

finovifi

KEY CYBERSECURITY CONCEPTS

CIA TRIAD

Confidentiality: Protecting sensitive data from unauthorized access (e.g., encryption).

Integrity: Ensuring data accuracy and trustworthiness (e.g., hash functions).

Availability: Ensuring systems and data are accessible when needed (e.g., DDoS protection).

DEFENSE IN DEPTH

Layered security approach (e.g., firewalls, intrusion detection, employee training).
AI and Machine learning in threat detection

ZERO TRUST MODEL

Verify every user and device, regardless of location (e.g., multi-factor authentication).

“Never trust, always verify”

finovifi

REGULATORY & COMPLIANCE CONSIDERATIONS

GLBA

(Gramm-Leach-Bliley Act): Requires protection of customer financial data.

PCI DSS

Secures credit card transactions.

FFIEC Guidelines

Emphasizes cybersecurity risk management for financial institutions

GDPR/CPRA

Protects customer data for banks operating internationally or in specific regions.

COMPLIANCE BEST PRACTICES

Conduct regular risk assessments.
Implement strong access controls and data encryption.
Maintain audit trails for all sensitive transactions.

finovifi

Practical Cybersecurity Meassures

Administrative Controls

- Regular employee training on phishing and social engineering.
- Develop and ***test*** an Incident Response Plan (IRP).
- Conduct penetration testing and vulnerability assessments.

Technical Controls

- Firewalls and Intrusion Detection Systems (IDS): Monitor and block malicious traffic.
- Encryption: Use AES-256 for data at rest and TLS 1.3 for data in transit.
- Multi-Factor Authentication (MFA): Require multiple forms of verification.
- Endpoint Protection: Deploy antivirus and anti-malware solutions.

Physical Controls

- Secure data centers and restrict access to critical systems.

BUILDING A CYBERSECURITY CULTURE

Employee Training

- Conduct quarterly phishing simulations.
- Educate staff on recognizing social engineering tactics.

Leadership Buy-In

- Ensure executives prioritize cybersecurity in strategic planning.

Customer Awareness

- Educate customers on secure banking practices (e.g., strong passwords, avoiding public Wi-Fi).

Continuous Improvement

- Regularly update policies and technologies to address evolving threats.

finovifi

INCIDENT RESPONSE BASICS

Steps of an Incident Response Plan:

1. Preparation: Establish policies, tools, and response teams.
2. Identification: Detect and confirm incidents using monitoring tools.
3. Containment: Isolate affected systems to limit damage.
4. Eradication: Remove threats and patch vulnerabilities.
5. Recovery: Restore systems and validate security.
6. Lessons Learned: Analyze incidents to improve defenses.

Example Scenario:

A phishing email compromises an employee's credentials.
Response: Disable the account, investigate the breach, and retrain staff.

finovifi

TOOLS & RESOURCES

Recommended Tools :

- **SIEM (Security Information and Event Management)** : Splunk, IBM QRadar for real-time monitoring.
- **Endpoint Detection and Response (EDR)** : CrowdStrike, SentinelOne.
- **Penetration Testing Tools** : Metasploit, Burp Suite.

Frameworks and Standards :

- **NIST Cybersecurity Framework** : Risk-based approach to cybersecurity.
- **CIS Controls** : 18 prioritized security controls.
- **ISO 27001**: International standard for Information Security Management Systems (ISMS).

Free Resources :

- CISA (Cybersecurity and Infrastructure Security Agency) guidelines.
- OWASP Top Ten for web application security.

finovifi

ACTIONABLE TAKEAWAYS

FOR BANKS

Perform a cybersecurity risk assessment within the next 3 months.
Implement MFA across all critical systems.
Schedule regular employee training and phishing simulations.

FOR CUSTOMERS

Use strong, unique passwords and enable MFA for online banking.
Monitor accounts regularly for suspicious activity.

PARTNER WITH EXPERTS

Work with trusted cybersecurity vendors for assessments and managed services.

finovifi

THANKS FOR YOUR ATTENTION!

Key Message:

Invest Train and Plan
Cybersecurity is an ongoing journey, not a one-time task.
Cybersecurity must evolve alongside digital offerings

Call to Action:

Start small, prioritize high-impact measures, and build a resilient security posture.

www.finovifi.com

cogle@finovifi.com

☎ 205.981.4424