SECUREYES
Infusing Security

Future-Proofing Your Bank

A practical guide for cybersecurity leaders to navigate the future of cyber threats, with insghts from leading central banks.

The Context.

In today's hyper-connected world, banks are prime targets for increasingly sophisticated cyber-attacks. As the financial sector becomes more digitized, the risks multiply, and cybercriminals are getting smarter, faster, and more persistent. Banks can't afford to be reactive anymore.

To survive and thrive, it's essential to take proactive steps toward cybersecurity - steps that not only prevent attacks but build resilience in the face of inevitable threats.

This guide is designed to help **senior leaders and cybersecurity experts** to navigate the future of cyber threats. We have compiled this document with insights from the guidelines laid out by regulators across the world.

Future of Cybersecurity Threats

ADVANCED PERSISTENT THREATS (APTS)

Cybercriminals will deploy sophisticated, long-term strategies to breach networks, especially targeting sensitive financial information

RANSOMWARE & MALWARE

Attackers use ransomware to lock systems and demand payments. Malware is increasingly used to extract critical financial data and compromise operations

INSIDER THREATS

Employees, either intentionally or through negligence, pose a growing cybersecurity risk. Insider threats can be difficult to detect and can lead to substantial damage.

THIRD-PARTY RISKS

Banks often rely on third-party vendors, which can be potential entry points for cyber-attacks. Monitoring these relationships is vital for security.

AI-POWERED ATTACKS

Cyber attackers are beginning to leverage AI to automate and scale attacks, making them harder to predict and defend against.

THE KEY STAKEHOLDERS OF CYBERSECURITY

1. Senior Management & Board
2. Chief Information Security Officer (CISO)
3. IT Teams & Cybersecurity Experts
4. Employees / Application Users

Senior Management & Board

ROLES AND RESPONSIBILITIES

- **Oversight & Accountability:** The Board is ultimately responsible for the institution's cybersecurity posture, including approving budgets and strategies.
- **Cyber Risk Framework:** Implement a comprehensive framework that aligns cybersecurity efforts with the bank's overall risk appetite.
- **Budgeting for Cybersecurity:** Allocate sufficient resources to continuously enhance cybersecurity infrastructure.
- **Review & Audit:** Conduct regular audits of cybersecurity practices and ensure compliance with regulatory guidelines.

Chief Information Security Officer (CISO)

ROLES AND RESPONSIBILITIES

- **Strategic Leadership:** Oversee the implementation of cybersecurity policies and ensure compliance with industry standards.
- **Incident Management:** Lead response efforts in the event of a cyber incident, coordinating with both internal teams and external partners.
- **Continuous Improvement:** Ensure that the bank adapts to new and emerging threats through ongoing risk assessments and training programs.

IT Teams and Cybersecurity Experts

ROLES AND RESPONSIBILITIES

- **Real-Time Threat Monitoring:** Implement real-time monitoring tools and practices to detect and respond to threats.
- **Patch Management & Updates:** Ensure all software and systems are up-to-date with the latest security patches to prevent vulnerabilities.
- **Access Control:** Implement strict access control measures, ensuring that only authorized personnel have access to critical systems.

Employees and Users

ROLES AND RESPONSIBILITIES

- **Cyber Hygiene:** Regular training programs should be mandatory for all employees, emphasizing the importance of strong passwords, phishing awareness, and reporting suspicious activity.
- **Insider Threat Mitigation:** Employees should understand the risks of insider threats and the importance of protecting sensitive data.

Steps to Build Cyber Resilience

ADOPT A ZERO-TRUST MODEL

Always verify users and devices before granting access to any network resources. This can mitigate insider threats and unauthorized access.

AUTOMATE THREAT DETECTION

Use AI and machine learning tools to automatically detect anomalies in network traffic, reducing the time to respond to attacks.

DEVELOP A CYBER CRISIS PLAN

Prepare a robust incident response plan, regularly updated based on evolving threat landscapes. Conduct regular drills to ensure readiness.

STRENGTHEN THIRD-PARTY RISK MANAGEMENT

Continuously assess third-party vendors for cybersecurity risks. Establish clear contractual obligations related to cybersecurity and data privacy.

FOSTER COLLABORATION

Encourage collaboration between banks, regulatory bodies, and cybersecurity experts. Share intelligence to stay ahead of potential threats.

Parting thoughts.

Cybersecurity is a shared responsibility.

Banks must not only comply with local regulatory guidelines but also adopt a proactive approach to anticipating and mitigating future threats.

Building resilience means creating a robust, dynamic, and scalable cybersecurity strategy that evolves with the digital landscape.

SecurEyes

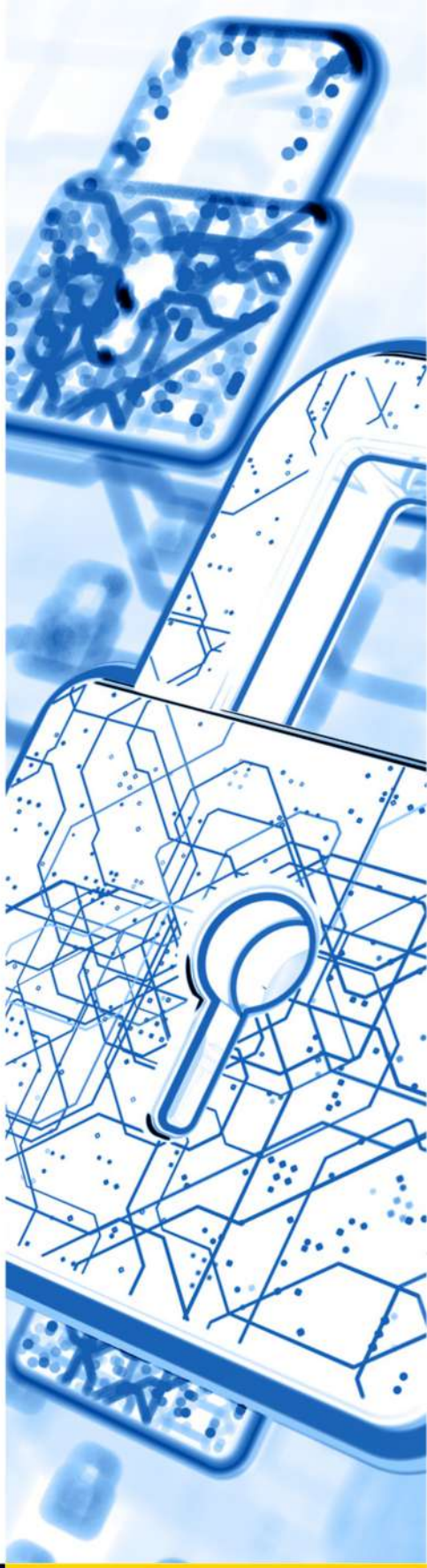
We help businesses stay ahead of the ever-evolving cybersecurity landscape by offering comprehensive solutions in risk management, regulatory compliance, and threat mitigation.

Whether you're looking for expert consulting services, cutting-edge products like vulnerability management and compliance tracking, or top-tier cybersecurity training through our academy, we've got you covered.

Let's secure your digital future together.

Contact us today for a tailored solution that meets your unique needs.

Get a Free Demo | Request a Quote



www.secureyes.net

IND +91 9939217654

IND +91 8041264078

UAE +971 50 8950797

USA +1 361 423 1683

hello@secureyes.net

SECUREYES

Infusing Security