ManageEngine
Log360

Security policy recommendations CISOs

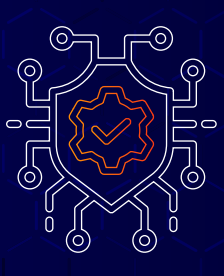
should consider to protect critical data against social engineering attacks

1 Vendor and third-party risk

- Implement a comprehensive vendor risk management framework with continuous monitoring.
- Mandate cybersecurity clauses in vendor contracts, including incident reporting timelines.
- Regularly audit vendors' security practices and their compliance with HIPAA/GDPR.

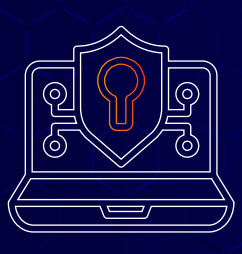
2 Identity and access security

- Enforce multi-factor authentication (MFA) across all systems, including vendor portals.
- Adopt zero trust with continuous verification of users and devices.
- Apply least-privilege principles with periodic access reviews.



3 Network and data segmentation

- Segment sensitive healthcare and financial systems from general IT environments.
- Implement micro-segmentation to reduce lateral movement opportunities.
- Maintain a real-time data activity monitoring system for abnormal access attempts.



4 Ransomware and double-extortion preparedness

- Build incident response playbooks for ransomware and extortion scenarios.
- Run regular tabletop exercises involving security, legal, and communications teams.
- Ensure secure, immutable backups are maintained offline for rapid recovery.

5 Threat detection and proactive defense

- Deploy advanced SIEM with UEBA for anomaly detection and insider threat visibility.
- Establish threat hunting teams to detect stealthy attacker behaviors.
- Leverage threat intelligence feeds to stay ahead of emerging attack vectors.

Additional security policy recommendations for CISOs to present to the board

- **Cyber insurance evaluation:** Explore coverage for ransomware, third-party breaches, and regulatory penalties.
- **Regulatory alignment:** Ensure continuous compliance with HIPAA, GDPR, CCPA, and upcoming healthcare security mandates.
- **Budget for cybersecurity resilience:** Allocate funding for 24/7 SOC operations, IAM enhancements, and vendor monitoring tools.
- **Cross-department collaboration:** Foster a culture of security awareness across HR, legal, and operations; not just IT.
- **Post-breach communication protocols:** Define clear escalation and communication pathways for regulators, customers, and the media.