C1

CYBERSECURITY STRATEGIES TO MINIMIZE THE RISK OF AI

More than 81% of respondents were concerned about the security concerns of generative AI.[1]

10-STEP PROCESS TO REDUCE AI CYBERSECURITY RISK

1
BUILD AN AI RISK MANAGEMENT PROGRAM
- Emerging AI Threats
- GenAI Technologies
- Policy & Governance
- Monitoring & Detection
- AI Training & Awareness

2
PERFORM AN AI SECURITY RISK ASSESSMENT
- Penetration Testing
- Simulated Attacks
- Threat Prevention
- Threat Detection
- Disaster Recovery

3
HARDEN YOUR SECURITY POLICIES
- Current Security Policies
- Data Classification
- Legal Compliance
- Third Party Policies
- Data Exposure & IP Protection

4
ENHANCE YOUR VULNERABILITY MANAGEMENT PROGRAM
- Inventory of Assets
- Vulnerability Scans
- Patch Management
- Compliance & Reporting
- Vendor Management

5
ENHANCE YOUR 24X7 DETECTION & INCIDENT RESPONSE
- Real Time Threat Detection
- Incident Response Planning
- Regular Updates & Drills
- Automate Responses
- AI-Based XDR

6
BUILD YOUR AI SECURITY VENDOR ASSESSMENT PROGRAM
- Vendor Assessments
- Key Assessment Criteria
- AI Security Best Practices
- AI-Based Security Solutions

7
BUILD A ZERO TRUST ENVIRONMENT
- Identity & Access Management
- Least Privilege Access
- Micro Segmentation
- Continuous Monitoring
- Encryption

8
BUILD A CYBER VAULT
- Cyber Recovery
- Clean Room
- Isolated
- Immutable
- Intelligent

9
MASTER YOUR ENVIRONMENT
- Network Topology & Data Flow
- Inventory of Assets
- Documentation
- Incident Response Plan
- Troubleshooting Skills

10
BE SKEPTICAL
- Question the Source
- Question the Intent
- Question the Impact
- Question the Urgency
- Question the Behavior

TAKE THE NEXT STEP IN REDUCING AI CYBERSECURITY RISK
Download C1's easy-to-use checklist at oneC1.com/AI-Risk-Checklist to start building an AI risk management program.

1. Stewart, A. (2023, September 21). Malwarebytes ChatGPT Survey Reveals 81% are Concerned by Generative AI Security Risks. Malwarebytes. https://www.malwarebytes.com/press/2023/06/27/malwarebytes-chatgpt-survey-reveals-81-are-concerned-by-generative-ai-security-risks