AI Impact Maine — ai-cybersecurity-guide (preview)

RESOURCE 9: ai-cybersecurity-guide

OVERVIEW

- **Audience:** All organization members
- **Primary Goal:** Security awareness + practical protection
- **Tone:** Urgent but not alarmist, empowering
- **Format:** Threat-focused + solution-focused

LITE VERSION (6 pages)

Page 1: Why AI Security Matters

- New threats AI introduces
- Real incidents
- Cost of breaches
- Your role in protection

Page 2: Top 5 AI Security Threats

1. **Data Breach**: Sharing sensitive data with AI
2. **Prompt Injection**: Malicious inputs to AI
3. **Model Poisoning**: Bad training data
4. **Privacy Leakage**: Unintended data exposure
5. **Vendor Compromise**: Service provider breach

Page 3: Protection Strategies

- What NOT to do
- What TO do instead
- Safe practices
- Spotting red flags

Page 4: Compliance Essentials

- GDPR implications
- HIPAA for healthcare
- FERPA for education
- CCPA for California
- Your industry requirements

Page 5: Incident Response

- What to do if breach suspected
- Who to contact

- Documentation
- Communication

FULL VERSION (40 pages)

SECTION 1: AI Security Landscape (5 pages)

- How AI systems can be compromised
- Unique AI vulnerabilities
- Difference from traditional cybersecurity
- Regulatory environment
- Industry trends

SECTION 2: Threat Deep-Dives (15 pages)

Threat 1: Data Exfiltration via AI - How it happens - Real examples - Detection signs - Prevention measures - Response procedures

Threat 2: Prompt Injection & Jailbreaking - Technical explanation - Real attacks - Warning signs - Defense strategies

Threat 3: Model Poisoning - What it is - How to detect - Impact - Prevention

Threat 4: Privacy Attacks - Re-identification - Membership inference - Model inversion - Defenses

Threat 5: Third-Party Vendor Risk - Supply chain risks - Vendor evaluation - Contracts and SLAs - Monitoring and auditing

Plus 3-5 additional threats

SECTION 3: Compliance & Regulatory (8 pages)

GDPR - Data subject rights - Privacy impact assessments - Data processing agreements - Breach notification

HIPAA - Protected health information - Business associate agreements - Risk assessment - Audit controls

FERPA - Student data protection - Parental rights - Disclosure requirements - Documentation

CCPA & State Laws - Consumer rights - Opt-out mechanisms - Security requirements - Reporting obligations

Industry-Specific - Financial services (PCI-DSS) - Government (FISMA, 800-53) - Utilities (CIP) - Healthcare (HIPAA, HITECH)

SECTION 4: Practical Security Guide (10 pages)

For Each Risk Category: - What to do - What NOT to do - Tools and technologies - Configuration guidance - Monitoring and auditing

Topics: - Data classification and labeling - Access controls - Encryption - Data retention and deletion - Vendor management - Incident response - Employee security training - Audit trails

SECTION 5: Vendor Security Evaluation (4 pages)

- Vendor security requirements
- Due diligence checklist
- Questions to ask
- Red flags
- Documentation needed
- Contracts and agreements

SECTION 6: Incident Response (3 pages)

- Detection and response plan
- Roles and responsibilities
- Communication procedures
- Documentation
- Post-incident review