Lemonade Cybersecurity Program

Enhancing Security, Protecting Assets, Building Trust

Team #42, Cybersecurity Consultant Company

- Introduction & Objectives
- **Timeline & Key Milestones**
- Budget Overview
- Resource Allocation
- Next Steps
- -Q&A

Primary Objectives:

- 1. Protect Critical Assets and Data
- 2. Support Al-Driven Innovation
- 3. Enhance Customer Trust
- 4. Ensure Operational Continuity
- 5. Achieve Regulatory Compliance
- 6. Foster a Security-Aware Culture
- 7. Manage Third-Party Risks

Purpose:

To outline Lemonade's strategic cybersecurity enhancements aligning with business growth and customer trust.

- Adopt cybersecurity framework Conduct initial assessments Assign leadership roles
- Phase 1: **Foundation** Building (Months 1-3)

Phase 3:

- Develop key security policies
 - Launch employee training programs
 - Implement basic security controls

Phase 2: Policy **Development & Training** (Months 4-6)

Comprehensive Controls & Deploy advanced Compliance security measures Conduct compliance (Months 7-9)

audits

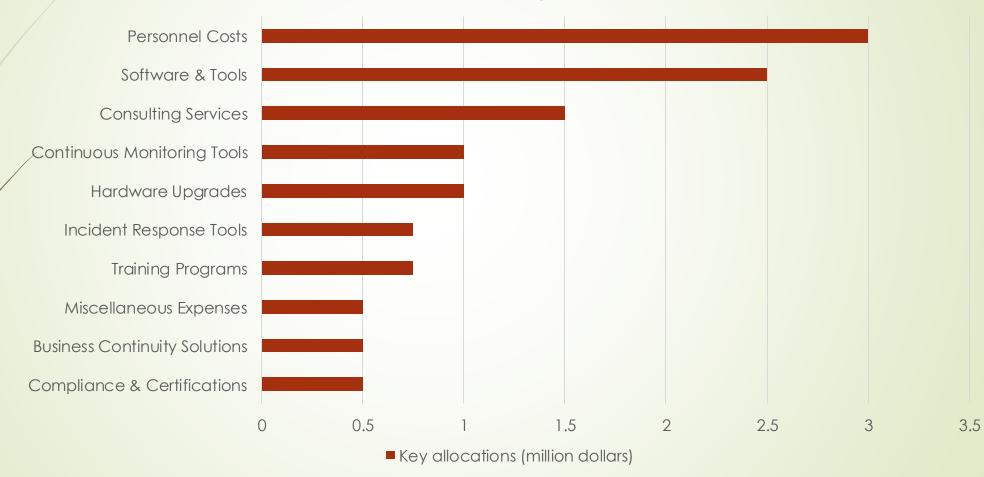
- •Secure third-party vendors
- Develop continuity plans

Phase 4: Continuous Monitoring & **Improvement** (Months 10-12) monitoring systems

- Implement ongoing
- Centralize asset management
- Refine incident response
- Regularly update policies

Budget Overview 🖔

Total Estimated Budget: \$10 Million



Resource Allocation 🞇

Internal Resources

Cybersecurity Team Expansion:

Hiring Security Analysts, Compliance Officers

IT Personnel:

Leveraging existing staff for security initiatives

Outsourced Resources

Consulting Firms:

Specialized tasks like compliance audits and advanced security implementations

Training Providers:

Comprehensive employee training programs

Next Steps 🚀



Questions?

We appreciate your time and attention. Your support is crucial in strengthening Lemonade's cybersecurity posture. Have any questions? We're here to help!

Team #42, Cybersecurity Consultant Company