Lemonade

Cyber Security Roadmap
2025-2028

Lemonade

- This three-year, $10 million cybersecurity roadmap will strengthen Lemonade's defenses against emerging threats and ensure global regulatory compliance.
- Key initiatives include AI-driven threat detection, robust vendor and supply chain security, advanced employee training, disaster recovery, and legacy system upgrades.
- These efforts will enhance data protection, operational resilience, and support sustainable growth, reinforcing stakeholder trust.

Risk Assessment

Lemonade

ID NO.	RISK or HAZARD DESCRIPTION	RESOURCES IMPACTED e.g., personnel, machinery	EXISTING CONTROL MEASURES	PROBABILITY LEVEL	IMPACT LEVEL	PREVENTION MEASURES
Garima	Loss of data	Entire business	No databackup process in place	High	High	Scheduling regular data backups: onsite and offsite; Creating a Disaster Recovery plan
Garima	Employee clicking on phishing links	Personnel, Data exposure	No SAT program in place	High	High	Creating and Implementing an SAT program
Christy	AI Data Poisoning	Entire business, AI-based sytems such as the Chatbot	Some; regular testing is done	High	High	Robust Data Validation; Anomaly detection algorithms, system audits
Christy	Not being in compliance with local regulations	Entire Business; incl. intl. scalability / expansion	Some, as business being done in some European countries	Medium	High	Observe frameworks: ISO cert (budget should allow), GDPR, NIST
Christy	Supply chain management risk	Entire Business and External Third-Party Vendors	No	High	High	Clear vendor regulation guidelines; Regulation compliance
Veronica	Missing assets or inventory/ Shadow IT	Entire business, Personnel, Stakeholders	No	High	High	Creating a Configuration Management tool (i.e. Service Now)
Veronica	Legacy systems running out of date software	Line of Businesses who are using EOL Legacy systems, Customers	No	Medium	High	End of Life planning for hardware and software to be defined in a
Veronica	Hardware failure and lack of disaster recovery	Entire Business, Customers, Stakeholders	No	High	High	Create a BCP and schedule DR exercise

Cyber Security Roadmap

Lemonade

	Year 1: 40% of Budget	Year 2: 35% of Budget	Year 3: 25% of Budget
Data Protection	Encrypt Data Implement DLP tools Onsite and Offsite backups	Expand and Automate Data backup strategies Continue enforcing encryption of all sensitive data	Implement comprehensive Data Governance Strategy for Integrity and Compliance Implement Advanced Anomaly Detection
Security Awareness and Training	Launch SAT program Email filtering and Anomaly Detection	Update SAT content based on emerging threats Advanced Email filtering	Utilize Advanced Simulations and Scenario-based Training Implement Adaptive Training Tailored to Employee Risk Levels
AI System Monitoring	Introduce data validation process and anomaly detection Validate training data sets	Implement anomaly detection algorithms Perform regular system audits	Predictive Analytics AI-driven detection algorithms
Compliance Frameworks	Implement GRC platform Begin ISO 27001 certification Develop clear vendor regulation guide lines	Automate compliance checks Continue ISO 27001 efforts Review & Enforce vendor compliance regulations	Perform continuous audits Finalize ISO 27001 certification
Configuration Management	Implement Configuration Management Database Enforce policies on unauthorized hardware and software use	Enhanced asset tracking to track real time updates Automate alerts for shadow IT systems	

Cyber Security Roadmap, cont.

Lemonade

	Year 1	Year 2	Year 3
System and End of life policies	Conduct system audits of legacy systems Create end of life policies Patch/Isolate/Upgrade legacy systems	Continue patching/isolation Replace legacy systems with modern tech aligned with EOL policy	Finalize replacement or decommissioning of legacy systems Rebrand Update Blog Design Update
TPRM and Vendor Compliance	Implement TPRM platform Establish vendor regulation guidelines	Mandate periodic audits for high risk suppliers Implement monitoring cybersecurity postures of key vendors	Social Media Campaign Blog Campaign Brand Change
DR and Business Continuity	Create DR and BCP plan with Recovery objectives Regularly backup critical systems Schedule DR exercises	Perform disaster recovery drills Update BCP based on lessons learned from DR exercises	Integrate AI-driven DR planning Conduct advanced simulations of hardware and software failure Ensure BCP is updated with infrastructure or regulatory changes

Anticipated Challenges

Lemonade

Challenge	Potential Impact	Mitigation Strategy
• Legacy Sys. Operations Continuity	• Vulnerabilities, Data Breaches	• Phased Replacement Schedule
• Comprehensive Compliance with International Regulatory Bodies	• Potential Fines, Reputational Damage, Operational Restrictions	• Automation Compliance Tools, Policy Review, Monitoring Team
• Vendor / Supply Chain Security	• Supply Chain Attacks, Disruptions	• Vendor Assessment Program
• AI Model Compromise	• Reputation, Data Integrity	• Validate Data. Anomaly Detection
• Sustained Employee Engagement in SAT programs	• Low Engagement = Exposure to Human Error Risks	• Interactive Training, Phishing Simulations, Incentivize Programs
• Balancing Budget with Security Goals	• Timely Execution of Key Projects, Risk of Vulnerability with Delays	• Quarterly Budget Review, Prioritize Projects, Optimize Costs

Key Deliverables

Lemonade

Year 1	Year 2	Year 3
• Automated onsite/offsite backups and a DR plan • SAT program rolled out with phishing simulations • Asset management through ServiceNow and end-of-life policies implemented • ISO 27001 certification efforts underway, aligned with NIST standards	• Regular DR exercises and backup strategies refined. • ISO certification progress tracked and nearing completion. • Real-time vendor security monitoring and compliance audits in place	• Finalized ISO 27001 certification. • Legacy systems replaced or isolated per the end-of-life policy. • AI-powered DR and BCP optimization.

KPIs and Success Metrics

Lemonade

- Backup Success: 95% success rate for data backup and recovery operations.
- Phishing Awareness: 60% improvement in phishing simulation response.
- Compliance: Achieve ISO 27001 certification and full GDPR compliance.
- Shadow IT: Eliminate 90% of shadow IT systems.
- Legacy Systems: Full replacement or isolation of legacy systems by Year 3.
- DR/BCP: 80% reduction in recovery times during disaster simulations