Clicked Team Sprint
Creating and Implementing a Cybersecurity Program (WiCyS)

Scenario:

Role: Cybersecurity Consultant
Company: Lemonade Insurance Company

You've been hired to come in on the cybersecurity team working for Lemonade. Lemonade, an online insurance company that covers everything from pets to laptops to your home, has been in the process of having an external team work on a cybersecurity program for them to implement. Being a small company, there was no program in place up until now. Lemonade is seeking out a comprehensive program that makes sense for their size and service offerings, most especially as they launched their AI model to predict catastrophes and claims, and uses that data to price their policies.

Company Concerns:

- Managing the development and maintenance of AI tools used for claims and incident predictions,and safeguarding the data they generate.
- Enforcing third-party security measures to ensure vendors adhere to best practices in data handling and protection.
- Ensuring full compliance with GDPR regulations to protect customer data across global operations.
- Strengthening the security of AWS SaaS cloud environments to safeguard customer and business-critical data.
- Developing and implementing a comprehensive Business Continuity Plan (BCP) to ensure operational resilience.
- Promoting adherence to company security policies by all employees through continuous training and monitoring.

Risk Assessment:

Risk Assessment for Lemonade Insurance Company

Objective: Prioritize risks associated with Lemonade's main concerns, identify vulnerabilities associated with these risks, and propose mitigation strategies.

AI-Powered Claims Prediction Tool

Risk: Exposure of sensitive customer data and susceptibility to AI-specific attack vectors, such as adversarial attacks or data poisoning.

- Assets:
  - Customer data used by AI to predict claims and incidents.
  - AI models responsible for decision-making and quote generation.
- Threats:
  - Data Breaches: Unauthorized access to customer data.
  - Data Poisoning: Malicious manipulation of AI training data to produce incorrect predictions.
  - Adversarial Attacks: Crafting malicious inputs that manipulate AI model outputs.
  - Model Inversion: Reverse engineering of AI models to infer sensitive data.
- Vulnerabilities:
  - Lack of secure SDLC for AI systems.
  - Incomplete logging and monitoring of AI model activity.
  - Weak encryption of data inputs and outputs.
- Impact:
  - High: A breach or malfunction in the AI system could lead to inaccurate quotes, customer mistrust, regulatory penalties, and reputational damage.
- Likelihood:
  - Moderate: AI attack techniques are increasingly sophisticated but may require specific expertise.
- Mitigation:
  - Implement a secure SDLC for AI systems.
  - Apply encryption for all AI data processing.
  - Deploy AI model integrity checks and monitor for adversarial behavior.
  - Regularly update and retrain AI models to mitigate the risk of adversarial data.

Cloud Security: AWS SaaS Platform

Risk: Unauthorized access to sensitive data stored and processed in AWS environments due to misconfiguration or compromised credentials.

- Assets:
    - Customer and claims data stored in AWS.
    - Cloud-hosted services for policy management, client interactions, and internal operations.
- Threats:
    - Unauthorized Access: Misuse of user credentials leading to AWS account breaches.
    - Misconfigurations: Weak IAM policies, or incorrect security group rules.
    - Insider Threats: Unauthorized internal access to sensitive AWS resources.
    - Denial of Service (DoS): Potential downtime affecting client services.
- Vulnerabilities:
    - Misconfigured IAM roles or overly permissive access policies.
    - Lack of continuous monitoring for unauthorized access or anomalous behavior.
- Impact:
    - High: A breach of cloud environments could expose sensitive client information and disrupt business operations.
- Likelihood:
    - Moderate: Cloud misconfigurations and credential compromises are common in SaaS environments.
- Mitigation:
    - Enable strict IAM policies with the principle of least privilege.
    - Enforce multi-factor authentication (MFA) for all AWS accounts.
    - Conduct regular configuration audits using tools like AWS Config and GuardDuty.
    - Implement real-time monitoring and alerting for unusual activity.

GDPR Regulatory Compliance

Risk: Non-compliance with GDPR and other global data privacy regulations, leading to legal penalties and reputational harm.

- Assets:
    - Personally identifiable information (PII) of customers across multiple regions.
- Threats:
    - Data Breach: Unauthorized access or misuse of customer data.
    - Non-compliance: Inadequate processes for obtaining customer consent, handling data subject rights, or transferring data internationally.
- Vulnerabilities:
    - Lack of formal data mapping and data subject rights management.

    - Insufficient customer consent mechanisms.
    - Potential gaps in data retention and deletion policies.
- Impact:
    - High: Non-compliance could result in significant fines (up to 4% of global annual revenue) and reputational damage.
- Likelihood:
    - Moderate: GDPR enforcement is rigorous, and Lemonade's global operations increase exposure.
- Mitigation:
    - Conduct a GDPR compliance audit to identify gaps.
    - Establish clear data retention, deletion, and consent policies.
    - Implement a formal process for handling data subject access requests (DSARs).
    - Ensure international data transfers comply with GDPR and other global regulations.

Lack of Business Continuity Plan (BCP)

Risk: Disruption of business operations due to unplanned incidents (cyberattacks, natural disasters) without a formal plan for recovery.

- Assets:
    - All customer-facing and internal business operations.
    - Critical IT infrastructure and cloud services.
- Threats:
    - Cyberattack: Ransomware or DDoS attacks that cripple operations.
    - Natural Disasters: Events like floods, fires, or power outages affecting data centers.
    - Supply Chain Disruptions: Third-party service or cloud outages.
- Vulnerabilities:
    - Absence of documented disaster recovery or incident response protocols.
    - Lack of redundancy in critical systems and services.
- Impact:
    - High: Prolonged service disruptions can lead to loss of revenue, customer churn, and reputational harm.
- Likelihood:
    - Moderate: The absence of a BCP increases the likelihood of extended downtime in the event of a major incident.
- Mitigation:
    - Develop a formal Business Continuity Plan (BCP) with defined RTOs and RPOs.

    - Implement disaster recovery mechanisms, including backup systems and offsite data storage.
    - Conduct regular BCP table top exercises to ensure effectiveness.

Third-Party Contractor Security

Risk: Exposure of customer or company data through third-party vendors who fail to implement adequate security measures.

- Assets:
    - Sensitive data accessed, processed, or stored by third-party contractors.
    - Lemonade's reputation and business continuity dependent on third-party services.
- Threats:
    - Third-Party Breaches: Data leaks due to inadequate vendor security.
    - Compliance Failures: Vendors not adhering to GDPR,ISO 2700, or other regulations.
    - Insider Threats: Malicious or negligent contractor access to sensitive systems.
- Vulnerabilities:
    - Inadequate vendor risk assessment processes.
    - Lack of contractual obligations or security standards enforced on third parties.
    - Absence of regular security audits for third-party contractors.
- Impact:
    - High: A breach or non-compliance by third parties could lead to legal penalties and customer data exposure.
- Likelihood:
    - Moderate: Third-party breaches are becoming increasingly common.
- Mitigation:
    - Perform thorough vendor risk assessments before onboarding new contractors.
    - Establish clear security requirements in vendor contracts, including data protection clauses and breach notification timelines.
    - Conduct regular security audits of third-party vendors and ensure they comply with security standards and regulations.

Lack of Formal Security Awareness Program

Risk: Increased likelihood of successful phishing attacks or internal threats due to lack of employee awareness.

- Assets:
    - Employee access to sensitive systems and data.
- Threats:
    - Phishing Attacks: Employees falling victim to phishing attempts that could lead to credential theft or malware infections.
    - Insider Threats: Unintentional data exposure or system misconfigurations by uninformed staff.
- Vulnerabilities:
    - Lack of formal training on common cybersecurity threats and best practices.
    - Insufficient communication on security policies and procedures.
- Impact:
    - Moderate: Phishing and insider threats can lead to data breaches or unauthorized system access.
- Likelihood:
    - High: Without formal and frequent security awareness training, employees are more vulnerable to common attacks.
- Mitigation:
    - Develop and roll out a security awareness training program focusing on phishing, password hygiene, and safe use of AI and cloud technologies.
    - Conduct regular phishing simulations and report on training effectiveness.

Security Policies and Procedures

Objectives:

Create a guide for implementing cybersecurity policies and procedures for Lemonade. Keeping in mind the companies concerns surrounding data protection, use of AI tools, cloud security, employee training, GDPR compliance, and third party vendors.

Frameworks:
NIST Cybersecurity Framework

Identify:
- All company assets (hardware, software, and confidential information)
- The mission and objectives of the company and build the cybersecurity program around it
- Current cybersecurity processes, policies, and procedures in place
- Risks associated with company assets/third party vendors and mitigation strategies

Protect:
- Company assets by implementing access controls (least privilege, sso,mfa, zero trust)
- Data, company reputation, and systems by developing a security awareness training program for all employees (new and existing) that is implemented on a yearly basis.
- Company data from theft, loss, or exposure from BYOD allowance (utilize a combination of MDM, MAM, UEM, VPNs)

Detect:
- Implement processes to detect threats and allow for automation
- Utilize continuous monitoring processes (XDR, SIEM, Firewalls)

Respond:

- Create playbooks to provide a standard for responding to potential threats.
- Perform tabletop exercises to ensure IR processes are up to date and efficient

Recover:
- Create a recovery plan that encompasses data recovery/loss and unexpected downtime)
- Create guidelines for communicating with customers/clients, stakeholders, third party vendors, and staff.

NIST AI Risk Management Framework

Map: Understanding Context and Risk Scope

- **Identify AI Use Cases:** Begin by mapping out where and how AI will be used in the business, like customer service, fraud detection, or inventory management.
- **Assess Stakeholder Impact:** Consider how AI impacts employees, customers, and other stakeholders. For example, if an AI system is used for hiring, the impact on applicants' privacy and fairness is crucial.
- **Define Purpose and Objectives:** Clarify the AI system's objectives and align them with the business's strategic goals. This includes understanding specific benefits (e.g., efficiency gains) and potential risks (e.g., biases).

Measure: Evaluating and Quantifying AI Risk

- **Develop Metrics and KPIs:** Set benchmarks to monitor AI performance in relation to risk factors like accuracy, fairness, and reliability. For instance, a fraud detection AI could be measured by its false positive rate, ensuring that legitimate transactions aren't overly flagged.
- **Test for Robustness and Bias:** Run simulations to evaluate how the AI performs in different scenarios, identifying potential failures or biases, such as how it performs across different demographic groups.
- **Implement Regular Monitoring:** Establish a continuous monitoring system to track AI performance and flag deviations. This is essential for AI systems that process data continuously, as it enables detection of changes or drifts in model behavior.

Manage: Implementing Risk Mitigations

Establish Incident Response Plans: Prepare for potential adverse outcomes by setting up a response protocol. For instance, if an AI-based recommendation system starts showing incorrect results, a mitigation plan should outline steps to correct it swiftly.

Maintain Compliance and Risk Controls: Ensure that the AI system adheres to GDPR for data protection by restricting data access, encrypting sensitive information, and conducting regular audits.

Automate Monitoring Where Possible: Automate the risk management process and set performance alerts for when unusual AI activity occurs.

Govern: Building a Governance Framework

- **Assign Accountability:** Establish clear roles and responsibilities for AI management within the organization.
- **Transparency and Documentation:** Maintain detailed documentation of model development, decisions made, risk assessments, and any incidents or corrections applied to the AI system.
- **Continuous Training and Audit Cycles:** Regularly train employees on AI use, monitoring, and risk management best practices.

Roadmap

Phase 1: Planning

Key Actions

- Perform a comprehensive risk assessment to identify critical assets, data flow, and potential vulnerabilities.
- Identify and map key stakeholders and contexts where AI is applied.
- Define security goals and objectives that align with Lemonade's business and regulatory requirements.

Alignment with NIST Frameworks

- **NIST CSF:** Identify
- **AI RMF:** Map (Understanding context, stakeholders, and impacts)

Challenges

- Gaining full visibility into AI-related assets and functions.
- Potential resistance to new policies and frameworks across departments.

Specialists Needed

- Cybersecurity Program Manager
- Risk Assessment Specialist
- AI Risk Consultant

Phase 2: Development

Key Actions

- Establish security policies for data protection, access control, and acceptable AI usage.
- Define AI risk metrics and set cybersecurity KPIs for performance and compliance monitoring.
- Create a policy framework specifically for AI data, model accuracy, and ethical considerations.

Alignment with NIST Frameworks

- **NIST CSF:** Protect
- **AI RMF:** Measure (Establishing risk metrics and performance standards)

Challenges

- Creating standardized KPIs for diverse AI use cases.
- Ensuring consistent policy implementation across teams.

Specialists Needed

- Policy Developer
- AI Specialist
- Data Protection Officer

Phase 3: Implementation

Key Actions

- Implement technical measures like access controls, encryption, and network segmentation to protect critical assets.
- Apply secure coding standards and practices for AI systems.
- Establish continuous monitoring systems for identifying AI and cybersecurity threats.

Alignment with NIST Frameworks

- **NIST CSF:** Protect, Detect
- **AI RMF:** Manage (Continuous monitoring and incident readiness)

Challenges

- Compatibility with existing systems and avoiding disruptions.
- Potential staffing limitations in monitoring AI systems continuously.

Specialists Needed

- Security Engineer
- Incident Response Team
- Network Security Specialist

Phase 4: Testing & Validation

Key Actions

- Conduct regular penetration testing on AI and IT systems to identify vulnerabilities.
- Perform audits to assess compliance with both NIST CSF and AI RMF.
- Run incident simulations to test response effectiveness for various scenarios, particularly in AI.

Alignment with NIST Frameworks

- **NIST CSF:** Detect, Respond
- **AI RMF:** Measure (Assessing robustness and resilience)

Challenges

- High costs associated with penetration testing and audit tools.
- Simulating real-world AI attacks or issues can be complex.

Specialists Needed

- Penetration Tester
- Compliance Auditor
- AI Testing Engineer

Phase 5: Incident Response

Key Actions

- Develop an AI-specific incident response protocol to address potential breaches or malfunctions.
- Set up real-time anomaly detection to monitor AI performance continuously.
- Define escalation paths and reporting requirements for AI-related incidents.

Alignment with NIST Frameworks

- **NIST CSF:** Respond, Recover
- **AI RMF:** Manage (Response and mitigation strategies)

Challenges

- Tuning real-time detection to avoid overwhelming alerts.
- Managing potential disruptions from false-positive alerts.

Specialists Needed

- SOC Analyst
- Incident Response Manager
- AI Monitoring Specialist

Phase 6: Training & Awareness

Key Actions

- Conduct cybersecurity awareness sessions, covering data handling, phishing, AI ethics, and data privacy.
- Offer technical training for specific teams to understand AI monitoring and incident response processes.

Alignment with NIST Frameworks

- **NIST CSF:** Protect, Detect
- **AI RMF:** Govern (Transparency, documentation, and training)

Challenges

- Ensuring training material stays relevant with evolving tech.
- Getting buy-in for continuous education across the company.

Specialists Needed

- Training Specialist
- AI Educator
- Security Awareness Officer

Phase 7: Governance & Review

Key Actions

- Conduct periodic audits to ensure compliance with updated standards and to capture improvement areas.
- Regularly review policies and metrics, updating as needed based on new risks or regulatory changes.

- Maintain detailed documentation for transparent, accountable decision-making.

Alignment with NIST Frameworks

- **NIST CSF:** Identify, Recover
- **AI RMF:** Govern (Assigning accountability, maintaining governance structures)

Challenges

- Keeping policies current with ongoing regulatory changes.
- Potential overhead costs of audits and documentation upkeep.

Specialists Needed

- Compliance Officer
- Governance Specialist
- Audit Manager

Cost Analysis

Objective:

The $10M budget is divided across key program areas, prioritizing must-have tools, staffing, and ongoing mitigation strategies, with considerations for adjustments based on critical needs.

Personnel Costs – $3,500,000

Hiring and training cybersecurity experts, risk specialists, and AI consultants.

- **Cybersecurity Program Manager:** $180,000 annually
- **Risk Assessment Specialist:** $140,000 annually
- **AI Risk Consultant:** $160,000 annually
- **Policy Developer:** $120,000 annually
- **Data Protection Officer:** $150,000 annually
- **Incident Response Team (3 specialists):** $420,000 annually
- **SOC Analysts (5 analysts):** $600,000 annually
- **Penetration Tester:** $150,000 annually
- **Compliance Auditor:** $130,000 annually
- **AI Testing Engineer:** $160,000 annually
- **Training Specialist & Security Awareness Officer:** $110,000 each annually
- **Additional Costs:** Training, certifications, and recruitment fees — **$500,000**

Tools and Technology – $3,200,000

Investments in AI and cybersecurity-specific tools, monitoring systems, and threat intelligence.

- **Security Information and Event Management (SIEM):** $500,000 (includes implementation and one year of licensing)
- **Endpoint Detection and Response (EDR):** $600,000 (for endpoints, licensing, and management for first year)
- **Threat Intelligence Subscription:** $400,000 (annual subscription for intelligence feeds and updates)
- **Penetration Testing Tools:** $300,000 (includes vulnerability scanning, DAST, and web app testing tools)
- **AI Model Monitoring Tools:** $400,000 (real-time performance and anomaly detection for AI models)
- **Cloud Security & AWS SaaS Management Tools:** $500,000 (covering AWS native tools, cloud governance, and security automation)
- **Data Encryption Solutions:** $300,000 (end-to-end encryption for sensitive data in storage and transit)
- **Backup & Recovery Systems:** $200,000 (cloud and on-premise backup, essential for Business Continuity Planning)
- **Additional Costs:** Installation, support contracts, and maintenance — **$200,000**

Compliance and Audit Costs – $800,000

Funding for compliance initiatives, audit preparation, and continuous assessments.

- **Annual Audits and Compliance Reviews:** $300,000
- **GDPR, CCPA, and ISO 27001 Certification Costs:** $250,000
- **Third-Party Risk Assessments and Vendor Audits:** $150,000
- **Policy and Documentation Management Tools:** $100,000

Training & Security Awareness – $500,000

Building a security-aware culture and keeping the team current with the latest cybersecurity trends and threats.

- **Employee Security Awareness Training (all employees):** $200,000 (including phishing simulations, data handling training)
- **Advanced Technical Training (cybersecurity team):** $150,000 (covering specialized skills like AI risk management and incident response)

- **Conferences & Continuing Education:** $100,000 (annual budget for industry events, conferences, and certifications)
- **Documentation & Training Materials:** $50,000 (for development, updates, and distribution)

Incident Response and Business Continuity Planning – $700,000

Preparation and readiness for responding to incidents and maintaining business operations.

- **Incident Response Playbooks & Protocols:** $150,000 (development, testing, and updating for real-world application)
- **Simulation Drills & Tabletop Exercises:** $100,000 (bi-annual simulations for incident response, including AI system failure scenarios)
- **Disaster Recovery Systems:** $250,000 (backup infrastructure, cloud redundancy, and response tools)
- **Incident Response Retainer (third-party service):** $200,000 (for additional support during major incidents)

Governance & Program Management – $600,000

Ensuring transparency, accountability, and ongoing governance of the cybersecurity program.

- **Policy Development and Review:** $150,000 (regular updates and reviews for regulatory alignment)
- **Governance Documentation Tools:** $100,000 (to maintain audit trails and record program changes)
- **Annual Program Evaluation & Metrics Analysis:** $150,000 (tracking effectiveness, compliance, and areas for improvement)
- **Dedicated Governance Specialist:** $200,000

Contingency Fund for Emerging Needs – $700,000

Allowance for unanticipated challenges, critical tool upgrades, or additional staffing needs.

- **Budget Flexibility for Tool Upgrades:** $400,000 (to cover essential upgrades or add-ons for key tools)
- **Emergency Staffing or Consulting Services:** $200,000 (access to specialized knowledge as needed)

- **Additional Training/Compliance Initiatives:** $100,000 (for emergent training needs or changing regulatory requirements)