4 YEAR Cyber Strategy and Roadmap Simulation

Business Goals and Objectives

1. **Strengthen Business Continuity and Disaster Recovery**
   a. Ensure operational resilience through updated BC/DR plans
   b. Establish robust incident response capabilities
2. **Achieve Compliance with Regulatory Standards**
   a. Attain and maintain compliance for GDPR, SOC, etc.
   b. Conduct regular audits and compliance assessments
3. **Optimize Operational Efficiency**
   a. Enhance asset management and internal processes
   b. Maintain documentation and improve cross-department collaboration
4. **Enhance Customer Trust and Engagement**
   a. Strengthen data protection and cybersecurity posture
   b. Develop and test customer communication platforms
5. **Develop Cybersecurity Awareness and Skillsets**
   a. Cultivate a culture of security awareness
   b. Upskill employees to meet evolving cybersecurity challenges
6. **Adapt to Emerging Threats**
   a. Continuously improve threat detection and vulnerability management processes
   b. Optimize detection systems to address the evolving threat landscape

Aligned Cybersecurity KPIs

1. **Strengthen Business Continuity and Disaster Recovery KPIs**
   a. Completion of BC/DR plan reviews and updates
   b. Time to recover from incidents
2. **Achieve Compliance with Regulatory Standards**
   a. Percentage of compliance assessments completed on time
   b. Number of non-compliance issues identified and remediated
3. **Optimize Operational Efficiency**
   a. Number of assets reconciled and documented
   b. Reduction in operational bottlenecks as identified through workflow reviews
4. **Enhance Customer Trust and Engagement**
   a. Deployment and testing of the customer communication platform
   b. Frequency of customer engagements providing cyber insights
5. **Develop Cybersecurity Awareness and Skillsets**
   a. Completion rate of awareness and training programs
   b. Skills assessments against defined roadmaps
6. **Adapt to Emerging Threats**
   a. Frequency and thoroughness of threat model reviews

Business Continuity and Disaster Recovery Metrics

- Percentage of BC and DR plans updated and approved by stakeholders
- Number of completed tabletop exercises vs planned exercises
- Recovery Time Objective (RTO) and Recovery Point Objective (RPO) achieved during simulated incidents

Compliance Metrics

- Number of compliance gaps identified and remediated per audit cycle
- Percentage of audit findings resolved within defined timelines
- Percentage of compliance reviews completed by the deadline

Operational Metrics

- Percentage of assets accurately documented and updated
- Number of cross-functional process improvements implemented
- Reduction in redundancy across workflows as measured by time and cost savings

Customer Trust and Engagement Metrics

- Customer satisfaction scores from cyber-related engagements
- Number of cyber insights or updates shared with customers through monthly or quarterly touchpoints
- Customer retention and trust index scored tied to cyber posture improvements

Awareness and Skillset Development Metrics

- Percentage of employees completing mandatory cyber awareness training on time
- Number of training sessions or modules delivered to employees, tailored to their roles

Emerging Threats and Detection Metrics

- Mean Time to Detect (MTTD) new threats from initial identification
- Mean Time to Respond (MTTR) to threats post-detection
- Number of high-severity vulnerabilities remediated within the defined Service Level Agreements (SLAs)

Y1: Foundational Development and Initial Implementations

Q1

Cross-Functional Relationships

- **Business Alignment**: Conduct initial alignment to understand what security needs to know about business processes
- **Compliance & Audit**: Appoint DPO/Privacy Manager and start research on compliance (GDPR, NIS2, etc.)
- **Program & Change Management**: Begin reviews of policies, business continuity plans, and disaster recovery plans

Cybersecurity Operations

- **Program & People Development**: Start implementing cybersecurity frameworks (NIST, CIS, etc.)
- **Asset Management**: Conduct an initial review and documentation of assets
- **Detection**: Select and implement initial monitoring tools
- **Emerging Threats & Vulnerability Management**: Establish a threat model and landscape

External Relationships

- **Partner Relationships**: Review 3rd party platforms
- **Customer Relationship**: Document communication and collaboration platform requirements
- **Public Relations**: Develop PR and crisis playbooks

Q2

- **Awareness & Training**: Start developing awareness and training programs tailored to business units
- **Compliance & Audit**: Prioritize and conduct additional compliance assessments
- **Cybersecurity Operations**: Establish internal tooling and workflows

Q3

- **Program & People Development**: Set metrics baselines and evaluate skills roadmaps
- **Detection**: Begin optimizing detection strategies based on initial implementations

Q4

- **Incident Response**: Develop incident response policies, plans, and playbooks; perform tabletop exercises
- **Asset Management**: Start ongoing asset management based on initial documentation
- **Customer Relationships**: Implement and test communication and collaboration platform(s)

Y2: Enhancements, Optimizations, and Compliance Reviews

Q1

- **Awareness & Training**: Roll out initial awareness and training programs
- **Compliance & Audit**: Start the initial audit; review compliance and regulation knowledge across teams

Q2

- **Program & People Development**: Focus on tuning the cybersecurity framework and adjusting the metrics
- **Incident Response**: Identify and implement IR tools, with tabletop exercises

Q3

- **Detection**: Conduct yearly review and adjustments to detection systems
- **Emerging Threats & Vulnerability Management**: Continue threat management and review threat models
- **Asset Management**: Conduct yearly asset reconciliation

Q4

- **Program & People Development**: Emphasize continuous improvement of hiring and skills development
- **Compliance & Audit**: Conduct compliance assessment

Y3: Maturity and Continuous Improvements

Q1

- **Compliance & Audit**: Continue compliance reviews and annual audit
- **Cybersecurity Operations**: Maintain ongoing resource optimization and documentation updates

Q2

- **Detection**: Optimize detection mechanism, incorporating new tools and methodologies
- **Incident Response**: Review and/or make adjustments based on prior incident response activities

Q3

- **Emerging Threats & Vulnerability Management**: Perform yearly review and threat management adjustments
- **Customer Relationships**: Provide insights through monthly and quarterly engagements

Q4

- **Communication Strategy**: Focus on regular, ongoing communication management and align strategies with business objectives
- **Public Relations**: Conduct a yearly review of PR and crisis playbooks

Y4: Optimization and Regular Reviews

Q1

- **Compliance & Audit**: Conduct compliance reviews and updates
- **Program & People Development**: Continue metrics optimization and framework tuning

Q2

- **Detection**: Continue detection optimization with yearly reviews
- **External Relationships**: Perform 3rd party and partner reviews

Q3

- **Incident Response**: Continue IR management and optimization based on regular assessments
- **Emerging Threats & Vulnerability Management**: Maintain ongoing threat management activities and optimizations

Q4

- **Program & Change Management**: Conduct comprehensive policy, tooling, and project management optimizations
- Complete annual (SOC) audit

Simulation

- Medium-Sized Company
- Security Staffing: One part-time or external security consultant with additional responsibilities distributed across IT staff
- Compliance Goals: Meeting basic regulatory requirements
- Tools: Basic security tools with incremental upgrades as needed

Detailed Breakdown by Category

- **1. Personnel**
  - Year 1: Part-time or outsourced cybersecurity lead + IT support allocation for security-related tasks.
  - Years 2-4: Incrementally increase personnel costs to account for either hiring a full-time cybersecurity specialist or expanding security responsibilities within the IT team.
- **2. Tools & Software**
  - Core Tools: Basic cybersecurity tools such as antivirus, endpoint protection, firewall, SIEM (Security Information and Event Management), and vulnerability scanning tools.
  - Year 1: Basic setup for essential tools.
  - Years 2-4: Gradual increase for enhanced tools, licensing, and upgrades as requirements grow.
- **3. Compliance & Audits**
  - Year 1: Initial compliance assessments (e.g., SOC 2 readiness, GDPR alignment), including appointing a Data Protection Officer/Privacy Manager.
  - Year 2-4: Increasing investment as compliance requirements mature, including annual SOC 2 audits, FedRAMP assessments, and continuous review costs.
- **4. Training & Awareness**
  - Year 1: Security awareness training for all employees, covering basics of cybersecurity, phishing, and data handling.
  - Years 2-4: Incremental increases for ongoing awareness programs, targeted training (e.g., role-specific), and management training for compliance updates.
- **5. Incident Response (IR)**
  - Year 1: Develop incident response policies, tabletop exercises, and basic incident handling procedures.
  - Years 2-4: Increase budget to implement IR tools, manage incidents, and conduct more frequent and advanced tabletop exercises.
- **6. External Consulting**
  - Year 1: Initial strategy development, compliance consulting, and threat modeling support from an external cybersecurity consultant.
  - Years 2-4: Additional consulting for audits, IR exercises, and continuous threat intelligence. Expect consulting costs to rise as the complexity of tasks increases.
- **7. Contingency**
  - Allocate approximately 10% for unexpected expenses, such as urgent tool upgrades, emergency incident responses, or additional consulting requirements.

Yearly Budget Breakdown

Category	Year 1	Year 2	Year 3	Year 4
Personnel	$80,000	$90,000	$100,000	$110,000
Tools & Software	$40,000	$45,000	$50,000	$55,000
Compliance & Audits	$20,000	$30,000	$35,000	$40,000
Training & Awareness	$10,000	$12,000	$15,000	$15,000
Incident Response (IR)	$10,000	$15,000	$20,000	$25,000
External Consulting	$15,000	$20,000	$25,000	$30,000
Contingency (10%)	$17,500	$21,200	$27,000	$30,000
Total Estimate	$192,500	$233,200	$272,000	$305,000

IT Budget Spent on Cybersecurity

- General Industry Average: 10%
- Technology, Healthcare: 13%
- Companies with a market capitalization of $300 million or less allocate a larger proportion of their budget (22.7%)

Source: Istari Global