Guide to Creating a Security Champion Program

1. Define the Objectives of the Program

Before launching a Security Champion Program, it’s essential to clearly define its purpose and goals. The program should align with the organization's broader security objectives.

Primary Objectives:

- **Promote a Security-First Culture:** Increase awareness and responsibility for security within all teams.
- **Decentralize Security:** Extend the reach of the security team by embedding security advocates in every department.
- **Identify and Address Security Risks:** Enable employees to identify and mitigate security risks early in their respective teams.
- **Provide Feedback:** Create a channel for security champions to provide feedback from their teams to the central security team.

2. Identify Roles and Responsibilities

Clearly define what it means to be a Security Champion and what responsibilities these individuals will have.

Typical Responsibilities:

- **Promote Security Best Practices:** Act as an advocate for security within their team, sharing guidelines, tips, and resources.
- **Provide Security Awareness Training:** Help their team stay updated on the latest security threats and prevention strategies.
- **Support Security Initiatives:** Assist in the rollout of security tools, policies, and procedures within their department.
- **Act as a Liaison:** Serve as the bridge between the central security team and their department, communicating security risks, incidents, or policy changes.
- **Monitor for Risks:** Help identify and report any security vulnerabilities or incidents that arise within their team.
- **Lead by Example:** Demonstrate best practices by complying with security policies and encouraging others to do the same.

3. Define Eligibility Criteria and Champion Selection

Determine how security champions will be selected and what qualifications or characteristics are required.

Eligibility Criteria:

- **Strong Interest in Security:** Candidates should have a passion for learning and promoting security practices, even if they are not security experts.
- **Good Communicators:** Champions should be able to communicate effectively with both technical and non-technical team members.
- **Leadership Skills:** They should be willing to lead by example and take initiative to implement security practices within their teams.
- **Cross-Department Representation:** Ensure that champions are chosen from various departments (e.g., engineering, HR, finance, marketing) to cover different aspects of the business.

Selection Process:

- **Nominations:** Ask managers to nominate employees who exhibit security awareness and leadership potential.
- **Volunteers:** Allow interested employees to volunteer for the role if they feel passionate about promoting security within the organization.
- **Central Security Team Review:** The security team should review and approve the final list of champions to ensure they meet the criteria.

4. Provide Training and Resources for Champions

Equip security champions with the knowledge and tools they need to be effective advocates for security within their teams.

Initial Training:

- **Security Fundamentals:** Provide champions with basic training on key security principles (e.g., password management, phishing detection, data protection).
- **Understanding Company Policies:** Ensure champions are well-versed in your company's security policies, procedures, and tools.
- **Incident Reporting:** Train champions on how to identify and report security incidents to the central security team.

Ongoing Support:

- **Regular Training:** Offer ongoing training on emerging threats, regulatory changes, and new security tools.
- **Access to Security Tools:** Provide champions with the necessary tools to monitor security within their teams (e.g., security dashboards, phishing simulators).
- **Resources:** Create a repository of security resources (e.g., guidelines, templates, checklists) that champions can use and share with their teams.
- **Champion Forum:** Set up a communication channel (e.g., Slack, Teams) where champions can collaborate, share insights, and ask the security team questions.

5. Create a Feedback Loop

Encourage continuous communication between the security champions and the central security team. Champions should feel empowered to share concerns, report vulnerabilities, and suggest improvements.

- **Monthly Check-ins:** Hold regular check-ins (e.g., monthly or quarterly) with all security champions to discuss ongoing issues, incidents, and new initiatives.
- **Feedback Mechanism:** Establish a formal process for champions to submit feedback to the security team. This could be through regular meetings, a feedback form, or an internal tool.
- **Champion Reports**: Ask champions to provide brief reports on the security posture of their teams, including successes, challenges, and potential security risks.

6. Establish Metrics for Success

Define key performance indicators (KPIs) to measure the effectiveness of the Security Champion Program.

KPIs to Track:

- **Participation in Security Initiatives:** Track the number of security champions actively involved in training, incident reporting, or leading initiatives.
- **Incident Reporting:** Measure the number of security incidents or vulnerabilities reported by champions and how quickly they are resolved.
- **Employee Training Completion Rates:** Track how many employees in each champion's department complete security training.
- **Phishing Test Performance:** Monitor the results of phishing simulations to see if departments with security champions perform better over time.
- **Employee Engagement:** Survey employees to gauge their awareness of security best practices and measure improvements over time.

7. Incentivize and Recognize Security Champions

Reward and recognize the efforts of your security champions to keep them motivated and engaged in the program.

Incentives:

- **Recognition:** Publicly acknowledge security champions during company meetings, in newsletters, or through internal communication channels.
- **Rewards:** Offer rewards such as gift cards, swag, extra time off, or professional development opportunities (e.g., security certifications, conference attendance).
- **Champion of the Month:** Highlight a "Champion of the Month" based on their contributions to the security program.

- **Career Development:** Provide champions with opportunities to advance their careers through additional security training or leadership development programs.

8. Continuously Improve the Program

The Security Champion Program should evolve as your organization and its security needs grow. Regularly assess the program's effectiveness and make improvements as necessary.

- **Annual Program Review:** Conduct an annual review of the program to assess its impact, identify areas for improvement, and adjust the program's structure or objectives as needed.
- **Champion Feedback:** Gather feedback from security champions on how the program is working for them, what challenges they face, and how the central security team can better support them.
- **Adapt to New Threats:** Update the program's focus as new security challenges or regulatory changes emerge. For example, if phishing becomes more prevalent, dedicate more training and resources to phishing prevention.

Summary

By implementing a Security Champion Program, a company can foster a proactive security culture, strengthen its defenses, and ensure that security awareness is integrated into everyday work. Empowering employees across all departments to take ownership of security will reduce risk and help the company maintain a strong security posture as it grows.