



Checklist 8 - Developing Cybersecurity Education Programs For Your Workers

Project Name: _____

Date: _____

Yes No

One of the strategies towards creating a cybersecurity awareness culture within your organization is by developing training programs/sessions for your workers to reinforce cybersecurity measures. In most cases, workers are the weakest links in the cybersecurity chain and as such, it is imperative that workers are enlightened on cybersecurity best practices such as appropriate data handling, safe internet usage, and identification of potential threats such as phishing, viruses, and malware awareness. Attackers and hackers are evolving and changing their tactics and as such, it is crucial to establish regular and on-going training sessions for your workers in order to be updated and foster increased awareness, avert risks, and ultimately enforce preventive measures. Developing cybersecurity training programs will enable workers to identify vulnerable spots and potential threats. This checklist therefore is a guide to developing cybersecurity training programs for workers.

Step 1 – Security Policies and Training Needs

1

Develop company-wide standards and policies regarding cybersecurity.

Notes



Checklist 8 - Developing Cybersecurity Education Programs For Your Workers

- 2 Check that all users are trained on appropriate usage of the organization's systems.

- 3 Prioritize employee cybersecurity training.

- 4 Establish clear definitions of IT usage.

- 5 Develop guidelines for safe internet usage and cybersecurity policies.

- 6 Establish penalties for violation of set guidelines.

- 7 Establish guidelines for data handling including customer info.

- 8 Evaluate your workers' training needs.

Notes



Checklist 8 - Developing Cybersecurity Education Programs For Your Workers

Step 2 – Developing Training Program

- 9 Develop a comprehensive program touching all cybersecurity bases.

- 10 Make the training program mandatory for all workers including leaders.

- 11 Ascertain your workers' cybersecurity capabilities.

- 12 Collaborate with IT specialists.

- 13 Base the training program on workers' roles and capabilities.

- 14 Enlighten workers on email and phishing malware.

Notes

Checklist 8 - Developing Cybersecurity Education Programs For Your Workers

15 Avoid a one-size-fits-all training approach.

16 Reinforce role-based training according to workers' skills and disposition.

17 Establish the most effective training approaches for detecting cyber threats.

Step 3 – Monitoring and Testing Capabilities

18 Conduct regular evaluations to ascertain workers' cybersecurity skills and knowledge.

19 Determine the effectiveness of the programs (is there a reduction in the number of cyber-attacks?).

20 Conduct mock cyber-attack exercises to identify vulnerabilities among workers.

Notes



Checklist 8 - Developing Cybersecurity Education Programs For Your Workers

- 21 Initiate fake self-phishing exercises with cues and lures to evaluate workers' skills or lack thereof.

Notes