Sr. No	List of topics to cover in cybersecurity awareness training
1	What are sensitive information and impact of that being stolen or misused
2	Password usage and management
3	Phishing
4	HTTP and HTTPs -> Importance of (S)
5	Corporate and Personal Smartphone usage security concerns
6	Low-tech hacking and social engineering
7	Secure email writing practices
8	Dumpster diving - Do not throw sensitive documents directly to trash/bin. Destroy it securely
9	Importance of 2FA/MFA (2-factor authentication/multi-factor authentication)
10	General security guidelines - Understanding of company policies and procedures - Escalation matrix
11	Malicious web surfing
12	BYOD security concerns
13	System and software updates
14	Importance of backup and storage
15	Usage of a secure network (Never use public Wi-Fi)
16	Privacy settings on a smartphone
17	Computer security basics
18	Malware, Spyware, Viruses, Trojans
19	Various types of Cyberattacks
20	Physical security
21	Data security
22	Remote access security basics (employees on travel)
23	Executive training on security awareness
24	Ransomware knowledge

Following is the list of tasks in order to flawlessly execute your high-end security awareness program.

#	Category	Task Name
1	**Preparation**	Find client through socialisation, business meetings, meetups, etc. Make them understand the importance of professional security awareness training
2		Prepare the communication plan with the client
3		Categorise and identify various training audience groups such as HR, Finance, IT, etc
4		Determine what security topics to be included in the training and assign one or more topics to a specific group of audience
5		Prepare the training content and deployment method
6	**Increasing your security awareness program efficiency**	Setup a dedicated security awareness team and appoint a team leader for the team
7		Develop security awareness policies to define program standards, frequency of training, processes and procedures to follow while deploying such training
8		Create a roadmap for the smooth transition, and this will allow you to deliver your training within the time limit
9		Setup a feedback form for end-users
10		Provided targeted training to each user groups
11		Provide interactive training by engaging users into individual and group activities
12		Take knowledge test exam of end-users to determine the outcome of your training. This will help you to identify improvement points for your training

13		Periodic phishing and spear-phishing campaign is must for any organisation
14		Occasional social engineering attacks should be carried away in the organisation
With the above preparation, either you can provide security awareness training within your organisation, or you can find a third-party vendor who can fulfil this for you		

For any security awareness program, measuring effectiveness, results and success of the program is mandatory. In order to identify your program delivery success, below things should be kept in mind.

#	Questionnaire
1	How many % of users attended training?
2	How many % of users successfully completed an entire training?
3	How many employees were using weak passwords?
4	What was the average time for each training carried within targeted groups?
5	How many users were posting sensitive company information on social media unknowingly?
6	What was the average end-user knowledge test score?
7	How many feedbacks/suggestions did you receive from your users?
8	How many % of users clicked on the phishing link?
9	How many % of users downloaded the attachment in the phishing email?
10	How many % of users entered credentials in the malicious phishing website?
11	How many % of users reported details of phishing emails to the IT or security team?
12	What was the average length of time it took for most of the users to fail a phishing test? (If real phishing attempt happens, an organisation should know their window to a response)
13	How many numbers of devices found unprotected within the organisation office?
14	How many users were a victim or multiple phishing emails?
15	How many reports of missing and stolen USB devices does your organisation get on a monthly basis?