TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

CYBER SECURITY *Training*

TIME TO GEAR UP YOUR HUMAN FIREWALL

TATA ADVANCED SYSTEMS
CYBER SECURITY PRACTICE

"As cybercriminals keep updating and embracing new tactics, tools and procedures to invade, the global workforce also needs to be apprised to security."

At the moment, cyber security training and awareness have become more important than ever for organizations. This topic has marked its seat in the board room discussions, specifically, when it comes to phishing attacks.

Companies have started investing in the training of their employees, instead of just focusing on the implementation of new security controls. In a recent survey done by Lucy Security in July 2020, around 96% of organizations agreed that cyber security awareness contributes to achieving a higher level of security. Furthermore, growing instances of data breaches and reputational damage across the globe are also encouraging enterprises to re-evaluate their security strategies and employees' cyber behaviour.

From Where To Start?

When it comes to efficient cyber security, the organizations must find answers to the following questions:

- Does each person in the organization know its cyber security responsibilities?
- Are cyber security roles appropriately assigned?
- Is there any structure for cyber security training and awareness in the organization?

Assess Your Workforce

Cyber security threats can come in any form or disguise – it could be an insider or external entity. Also, humans errors are accounted for a majority of security breaches. So, it becomes more crucial to conduct a comprehensive assessment of your workforce (before beginning the training) to check their level of awareness and knowledge.

This assessment can provide organizations with a brief about how employees' react to adverse situations, which could be anything ranging from a phishing attack to social engineering. They can even identify if employees are following safe password practices or using same and weak passwords on multiple applications.

TATA ADVANCED SYSTEMS
CYBER SECURITY PRACTICE

Plan Training Post Assessment

Once the assessments are done and results are analysed, companies can program and schedule the cyber security training and awareness sessions accordingly. Results can help them to determine the most relevant topics that can be prioritized and focused during the session. The training areas may include (but not limited to) the following:

- Social Engineering
- Phishing
- Strong Passwords
- Identification of Security Risks
- Compliance Issues

This assessment is expected to help organizations a lot as an effective security approach should not be limited to what an employee must know, instead, it must also focus on what they should do. Such assessments should be done for all employees at every level inside an organization.

Encourage Cyber Security Awareness & Training as Culture

Creating and maintaining a cyber security culture within an organization is a continual process that needs to be executed in a timely manner. It is not mandatory to use high-tech solutions always, "awareness and training programs" can help you in getting started with the process. You just need to make it interesting for people, which can be done through different communication channels. These channels may include, but not limited to:

- Monthly campaigns with powerful slogans
- Creating some exciting videos
- Useful blogs highlighting security awareness
- E-newsletters for quick sharing of information
- Creative banners or posters displaying security tips
- Monthly workshops with real-time simulation

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

Benefits of Conducting Cyber Security Training

The efficacy and success of any training program depend on how it is implemented. A well-designed cyber security training session can elevate the level of the overall security and reduce the chances of a potential cyber attack.

Let's have a look at some other advantages of an effective cyber security training program.

- Incorporates security values into the roots of your business
- Minimizes the probability of a successful security breach
- Helps in achieving regulatory compliance and improving the audit results
- Strengthens the cyber security posture
- Boosts relation with customers and partners

Towards The End...

As cyber threats are evolving rapidly, our dependence on cyber security has soared accordingly. Increased usage of internet and mobile devices have made us more vulnerable than ever before. If we talk about the businesses, a single cyber security breach can cause irreversible damage and bring a company to its knees. Therefore, security awareness and training programs have become vital for organizations. Educating the workforce about different threats can reduce the risks to a greater level.