TATA

TATA ADVANCED SYSTEMS

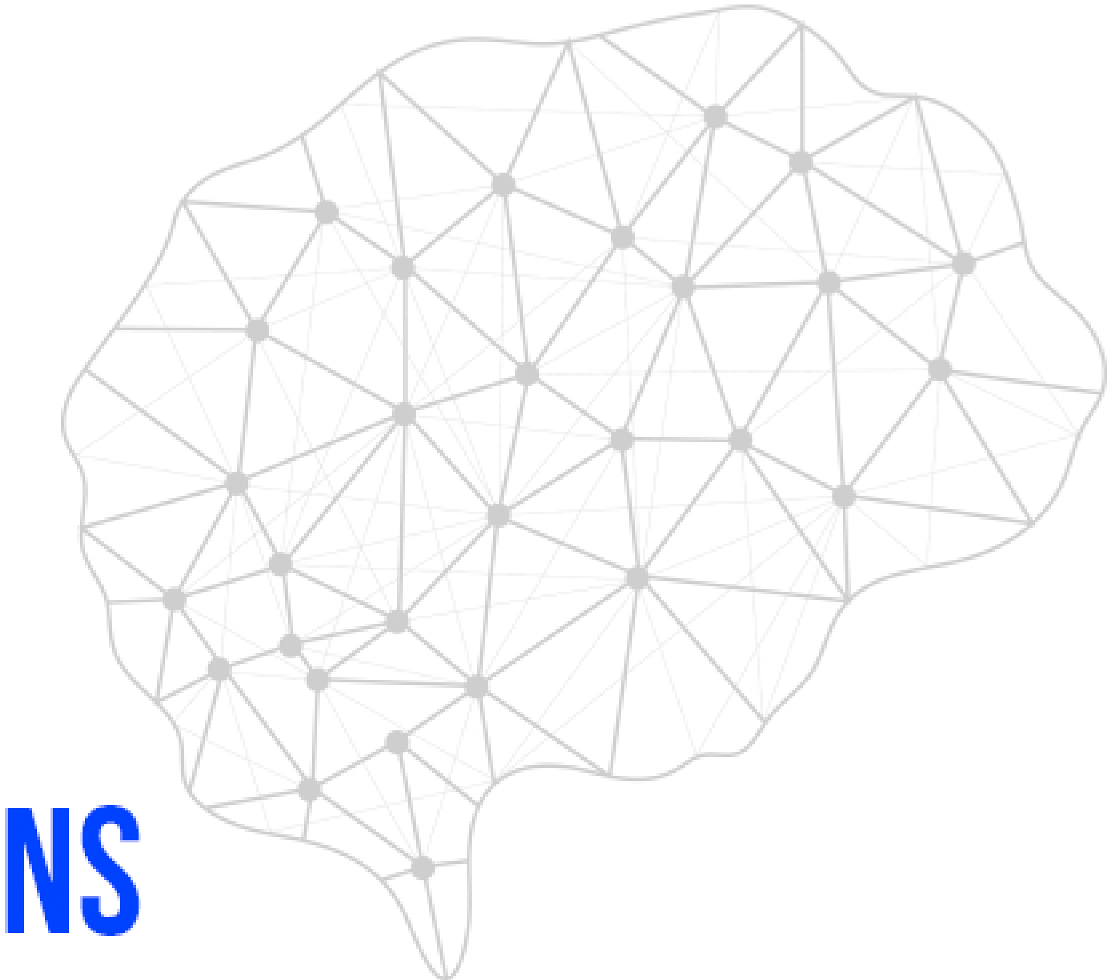
CYBER SECURITY PRACTICE

SECURING THE MOST VULNERABLE ASSET - HUMAN

Follow us: @tataadvanced

Humans are viewed as the most susceptible link in the People-Process-Technology triad. Despite having robust security solutions like Intrusion Detection Systems (IDS) or firewall, your weakest link could let attackers bypass the security controls. Cybercriminals always take advantage of the fact that people are more likely to create mistakes, which could be intentional, unintentional or lack of action. According to the Human Factor 2019 report, 99% of cyber-attacks require some level of human interaction to execute.

Trends like flexible working and personal device usage amidst the new normal have completely changed user behaviour. It has also observed that most of the employees do not restrict their family members and friends from accessing their work devices that may create a myriad of cybersecurity risks for organizations. That's why most of the security professionals think that inattention among employees for security practices is putting the enterprises at risk. They believe that employees can easily misuse their access to reveal, erase or alter the business-critical information. As per the 2020 Data Breach Investigation Report from Verizon, 30% of breaches involve internal actors. This indicates and proves (to a great extent) that insider threats pose a significant risk to the cybersecurity of an organization.



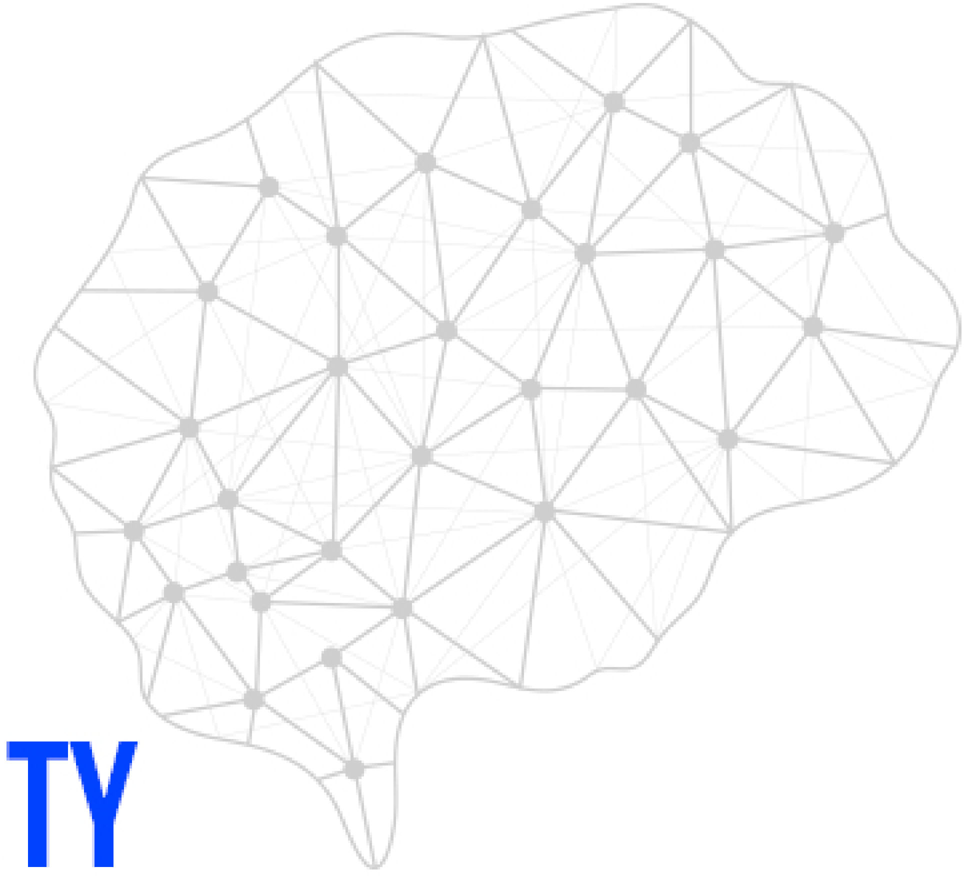
HOW CYBERCRIMINALS TARGET HUMANS

Phishing, Social Engineering & Business Email Compromise are the most common cyber threats posing a serious concern for organizations globally. These attacks have a high success rate as humans are the first contact point. Let's have a close look at each cyber threat.

- Targeted Phishing attacks have increased at an incredible speed since businesses have started to continue operations remotely. The remote locations do not have adequate security measures in place to counter the ongoing threats, which make employees more prone to cyber risks. Cybercriminals are leveraging the current situation by flooding remote workforce with COVID-19 themed phishing emails intending to steal credentials, data and gain access to critical business resources. They are also imitating the most renowned brands like Apple, PayPal & Netflix to launch phishing campaigns.

- Social Engineering is another common method used by attackers to target people and businesses. It involves human psychological manipulation to trick them into making mistakes like giving credentials to access corporate data/systems, providing critical information, etc. This attack generally happens in several stages. Initially, cybercriminals gather required information about the target through social media websites like Facebook, Twitter, LinkedIn, Instagram, etc. Then, they establish a relationship with the target. Once the trust is built, they communicate further to exfiltrate the data.

- Business Email Compromise (BEC) is the most sophisticated form of phishing that utilizes social engineering tactics to manipulate and trick victims. The attackers implement techniques like display-name spoofing, domain spoofing and lookalike domains to execute BEC attacks. These attacks revolve around impersonation in which the attacker takes over the email account of someone the victim trusts. This could be a senior-level executive of the same organization or a trusted counterparty. When the victim receives the email, it seems like a legitimate & usual business request. Consequently, the victim processes the request without having any idea about what is going on in the backend.



HOW TO MITIGATE HUMAN VULNERABILITY

Recommended security controls can be followed to mitigate the risk of employees becoming the victims of cyberattacks:

1. Initiate a security awareness program to enhance security, reduce errors and prevent damage to brand reputation.
2. Identify your VAPs (Very Attacked People) as they highlight significant areas of risk to the business.
3. Conduct a regular risk assessment of employees to mitigate cyber risks.
4. Provide in-depth security training to help employees recognize phishing emails and other growing cyber threats.
5. Encourage employees to follow best practices of proper password management.
6. Actively manage and monitor the privileged accounts of your organization.
7. Appreciate those who follow proper cybersecurity hygiene throughout the organization.

The need of the hour for organizations is to follow a people-centric cybersecurity approach that must include an effective security awareness program. Investment in the training of employees will make them aware of the increasing cyber threat landscape and help them to react accordingly if they are hit with a cyberattack. Also, improving cybersecurity understanding among employees will assist organizations to meet the regulatory compliance.