Behaviour Change Game

Designing Effective Security Awareness Programme to Fortify your Human Firewall

Author: Ashish Shrestha, Co-Founder of Stupa Infosec

'Linking Information Security to Digital Wellbeing'

March 2022

MERITEC
Talent & Technology

stupa
VISION BEYOND PROTECTION

Meritec Ltd are delighted to have partnered with Stupa to deliver our new Cyber Security E-awareness course. This new approach that we have taken together to provide awareness to all organisations around cybercrime fits well with Meritec's core principle of providing cost-effective digital solutions.

The latest version of the product contains up-to-date information on how cyber security awareness across the organisation can help to protect your employees and the organisation from the inwards, outwards. The course is designed to empower your employees with knowledge that goes beyond the office and delivers a broad and consistent level of understanding of cyber security in around 45-60 minutes. The course was developed in conjunction with Stupa.io and provides key messages in a non-technical, easy-to-understand way.

The following white paper was created by Ashish Shrestha, Co-Founder of Stupa Infosec, Information Security Leader Linking Information Security to Digital Wellbeing. Ashish has created this whitepaper to allow a deeper dive into all things cyber including security defence systems, problem-solving, and finding a new approach to cyber security (and much more!). We are very excited about our partnership with Stupa, and we feel very positive about how we can help build a safe place online for all organisations, together as a team.

'Raise awareness and reduce risk by empowering your employees to improve their Cyber Wellbeing with Meritec Cyber Security E-Awareness Training.'

Foreword

There is no doubt that the “Human Firewall” are the best security defence system that ever exists. Yet, we see a vast majority of Security Awareness Training (SAT) programme strategies continue to fail in achieving the desired outcome or only get limited results. So why is it despite all the effort and advancements in technology, and fancy presentation slides, it is difficult to permeate the human mindset and inflict the desired change in their behaviour and culture within an organisation? Who is at fault here – Information Security programme, business technology in use or the employees?

We need to step inside the problem with an intention to solve it because going out of the problem is not the solution. And I am going to say something counterintuitive, and some may even find it provocative. Furthermore, some of us might disagree too, but nonetheless, here is my thought – It is the status quo on how we have crafted and delivered the awareness and training in decades in a stereotypical manner that is the weakness in Information Security Awareness Programme, not human. Truth is bitter but it still stays true.

A classroom style, death by PowerPoint shoehorned to broadcast company policies – Do’s and Don’ts – Capitalising on fearmongering, carrot vs beating stick approach fuelled by disciplinary action on non-compliance that is stupid, and not human. Let’s face it, this policing control and warden like behaviour simply does not work. As matter of fact, it frustrates humans.

Perhaps, I am about to say something even more provocative here, but in my opinion, it is the years of experience of the leaders in this domain on pressing to instil security discipline in a traditional way by scaremongering and promoting beating stick approach is the core of the problem. And honestly speaking I believe is the single most factor in imprisoning and impeding the desired progress and outcome.

Put simply, the traditional approach does not have the lens and required depth to understand that the SAT is less about content, not about promoting bad news nor banking on the fear factor, but more about human behaviour and storytelling and tapping into emotions. We are not looking inside the box for the problem to change the outer reality but fixated with a conservative mindset and the hypothetical problem statement – “Human is the weakest link in the cyber chain”. This is wrong!

Table of Contents

1 Adopt a Problem First Vs Solution First Option **p 1**

- **1.1** Learned Moments
- **1.2** Unlearned Moments
- **1.3** Relearned Moments

2 Our Approach Must Change **p 5**

3 Adopt a Clear Purpose and Maintain Focus **p 6**

4 Educating Beyond Compliance Gap **p 7**

5 Contact Us **p 8**

1.

ADOPT A PROBLEM FIRST VS SOLUTION FIRST APPROACH

What has been your approach and remedy to this? You may ask.

I'd like to share with the readers my **Learned**, **Unlearned,** and **Relearned** moments.

1.1.

Learned Moments - Applying the same approach to the same problem is not a solution - Be relentless about finding a new approach

To begin with, I had to begin my journey with **"Learn"**. This journey started with intense research and meticulous analysis - Books, articles, and publications about creating an impactful change. Not only that but learning to understand the basic science behind the human brain and the associated neuroplasticity.

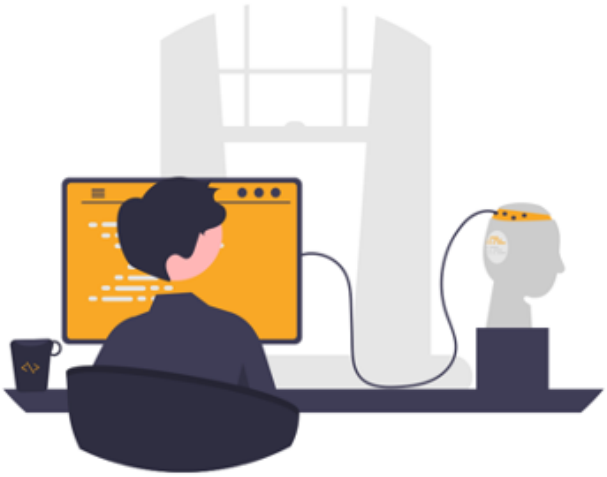
More importantly, then implementing these learning moments in bite-size manageable chunks. Assess and install these "Learned" principles to the practicality to try and be creative in inspiring the security culture change transformation within the organisation. It worked, it honestly did. You see, the human brain is a sophisticated piece of biological technology and me being a technology fanatic, the more I researched the more it got me fascinated.

I soon learned that behaviour change pattern does not happen because of rational scripture I try to inject into my audience. It is not a computer system that we can program to create a robotic operation under our command and control.

I learned that to really trigger true behavioural change the part of the complicated human brain that is designed to make “logical decisions” must be the target vs rational brain system. This part of the brain controls feelings, values, and emotions. I then had another learning moment that this part of the brain does not understand languages or scripture. No wonder the classroom style or the policy-driven programme does not yield the desired success.

I understood that to acquire the attention, retention, and action from my audience, I needed to design a program that can tap and speak to human emotions.

Furthermore, behavior change is elusive in nature, and to achieve your desired programme objective and key results, you need depth, authenticity, and a true desire to make an impact. And to make an impact you must immerse yourself in the process.



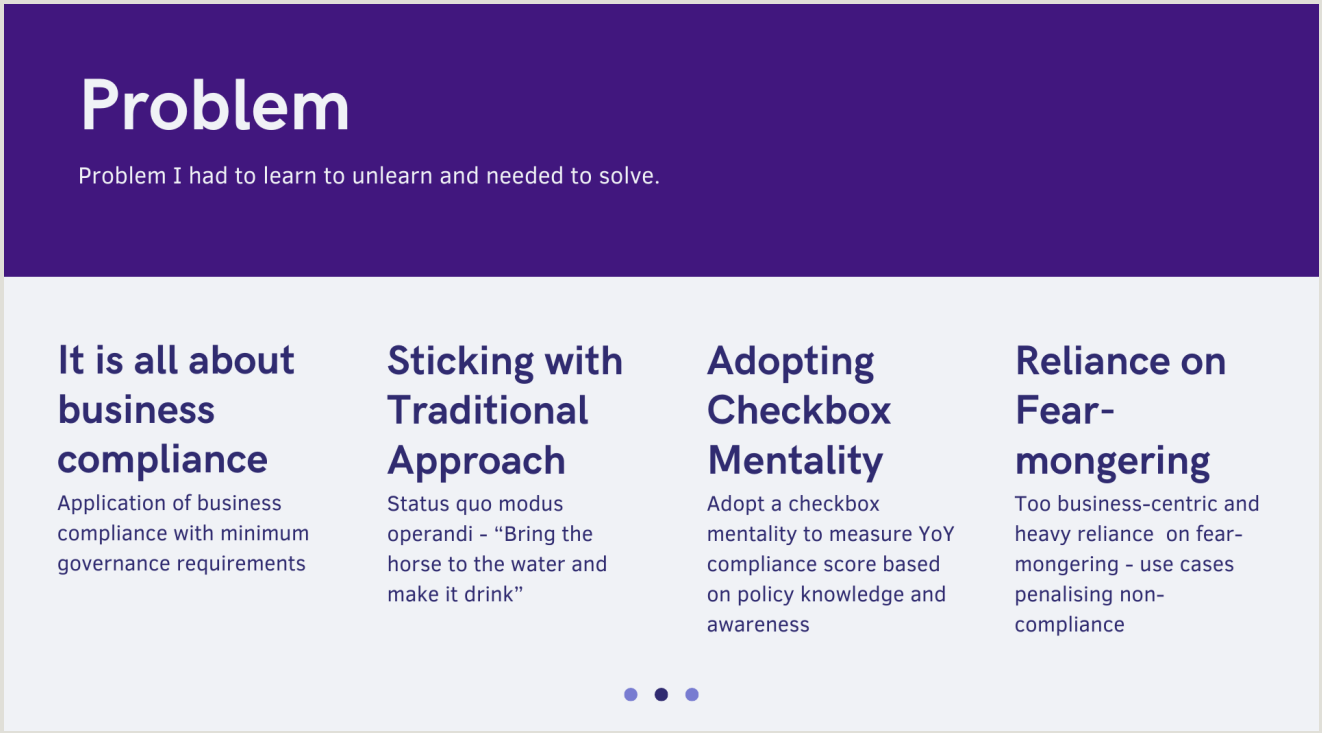
I can reassure you that it certainly yields better outcomes than the conventional stereotype training techniques.

This aspiration of change involved a process of destructing my old habits to install the new ones. I had to **“Unlearn”** and let go of the approach and problem that even I was part of and leading it.

1.2.

Unlearned Moment - Experience does not equate to simplicity and pragmatism (not always)

In my more than a decade of experience in this domain, I have seen, been part of, and executed many SAT programmes with deluded optimism to instil basic cyber security hygiene practice within their business and drive culture changes based on below:



In this segment of unlearning, my learning also came with discovery and realisation that there is huge fatigue amongst people who are the biggest asset for the success of the business when it comes to the learning programme.

The only issue here is that the above is not only counter-productive to truly building a pragmatic nut , it is also not a sustainable programme strategy when it comes to supporting and fortifying with the right cyberculture that delivers.

Designed to broadcast business/corporate rules in dictatorship style - Never ending list of Do's and Don'ts

Celebrating the success of the programme on victimising the people and capitalise on these statistics

Use the above statistics to enforce disciplinary action and further fearmonger

1.3.

Relearned Moment - Be creative in generating the thirst in your audience

As I have previously insinuated that the core of the challenge appears to be as much of a biological problem that we have as humans along with a poorly designed awareness and training programme that is inflammatory to this problem. Yes, you read it right – A neurobiological battle that needs to be understood and conquered!

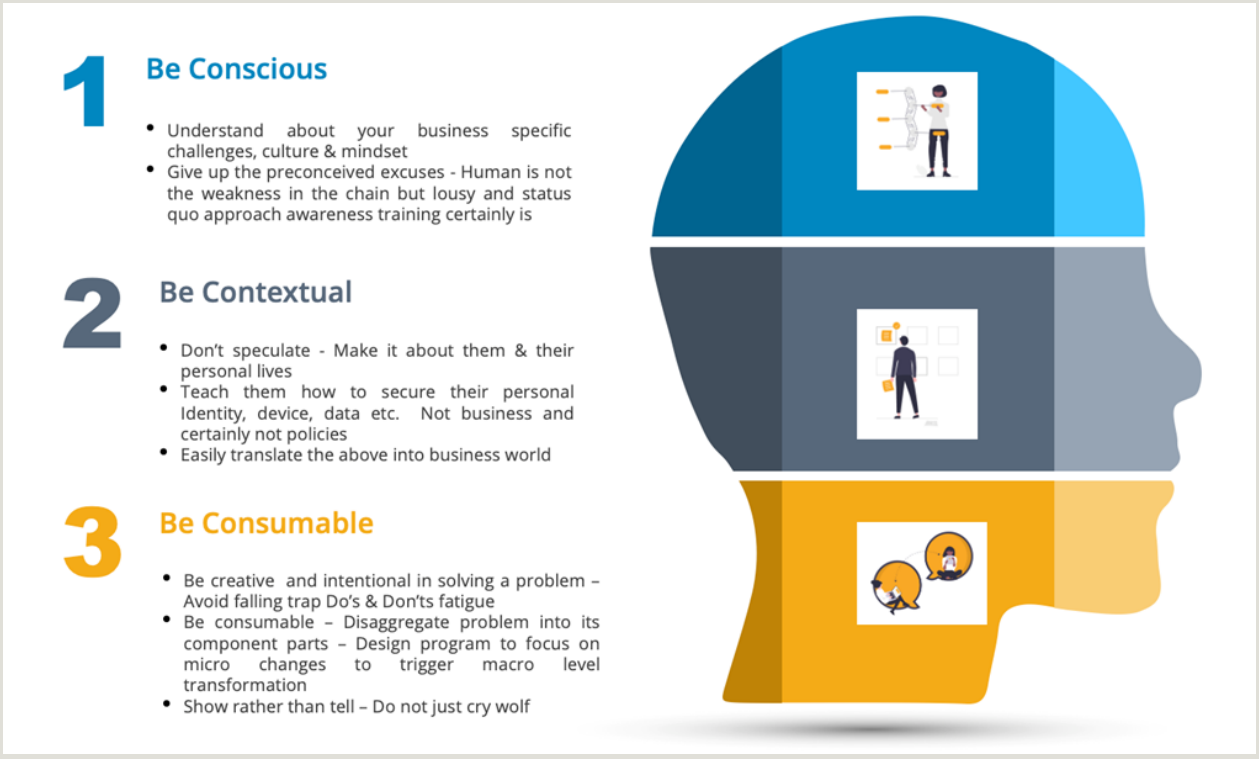
Most of the security awareness programmes out there is talking about building and changing “Mindset”. But criticality of the solution to the problem lies in focussing on the change of the “Emotionality” – Why do we (humans) think and behave the way we do?

I unlearned the status quo to relearn that being conscious and contextual in communicating “WHY” is it important for them, and not the business and brand reputation and growth is critical in generating the thirst – The curiosity to get themselves to the oasis in the first place. “How” and “What” of the strategy is secondary, and in fact comes naturally as a by-product of this thinking.

Treating them less machine-like and more human-like is the sole element I needed to develop the programme that can grab the “Attention” of your audience - “Retain” the attention, information and inspire the application of desired “Action”. Mindset change becomes the by-product of this winning mantra.

2.
OUR APPROACH MUST CHANGE

For me designing a radical, successful, and enduring SAT Programme has revolved around my **3C Principles:**



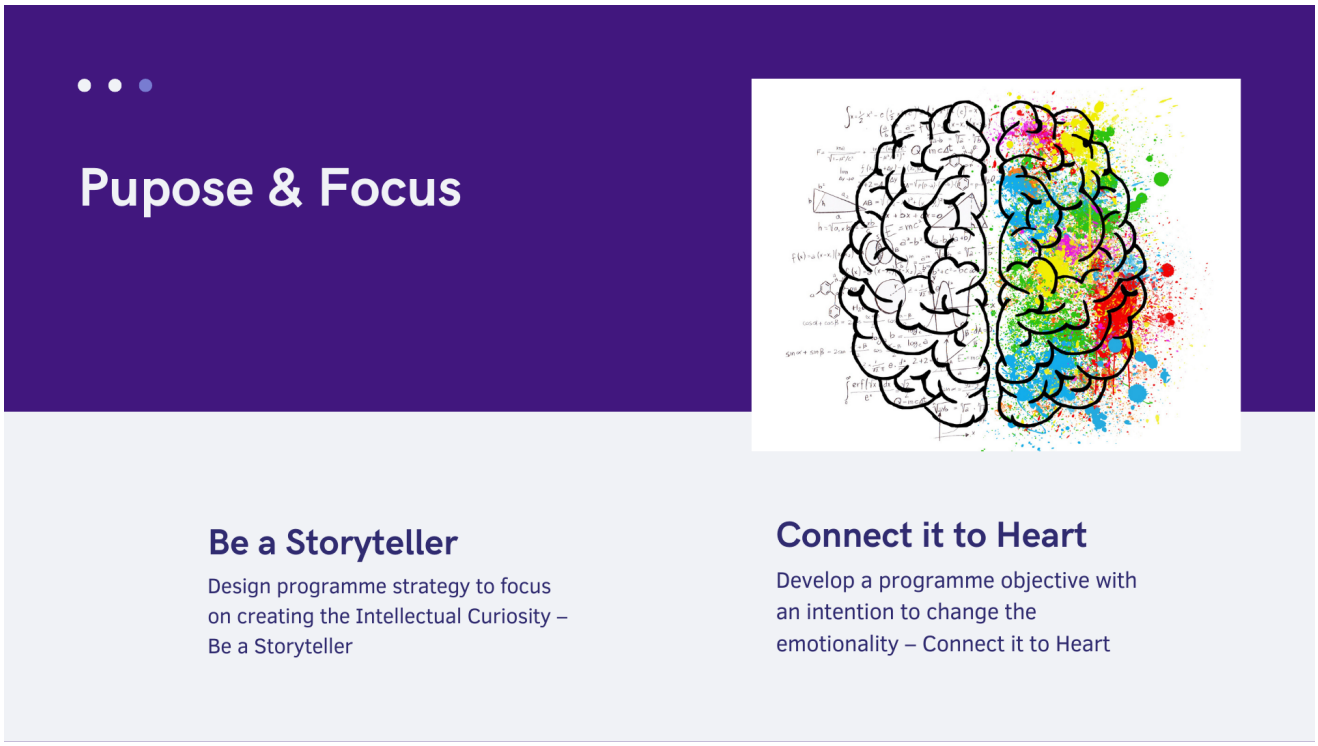
It should also be noted it is not only paramount to keep it "fun and entertaining" but also it is important that you "test your program's effectiveness, not people". As the adage goes - Trust but verify – Conduct attack and active breach simulation.

3.

ADOPT A CLEAR PURPOSE AND MAINTAIN FOCUS - IT CERTAINLY IS YOUR COMPASS IN THIS JOURNEY

It is optimistic to even try and cover everything on this topic in this article but it is important to understand that maturity is a journey and an evolution in building a sustainable programme. I am still continuing to learn to unlearn and relearn on a continuous basis.

The whole objective here is to shift your compass to help maneuver and to not lose track of your true purpose and focus.



The fundamental problem we are facing is because we believe that our job is to take the horse to the water and make them drink - We are not creating thirst. But if we can make someone thirsty you never have to take them to water or make them drink. They will find their own water and then drink all their lives. This is what I call intellectual curiosity.

Furthermore, it is not news that “Human” is sociable by nature– We love attention – We are emotional beings and have feelings - We love things simple and fun – We love things broken down into consumable and relevant context – Focus on micro action to drive macro-level changes.

This simple recalibration can help repair and reinforce a security awareness program that makes the human mindset and behaviour shift.

Maintain laser-like focus on “Why” that’s your programme vision, be relentless about “How” you can bring different, creative, and innovative, and cleverly connect it to “What” in terms of your audience benefit first, and not business.

4.

EDUCATING BEYOND COMPLIANCE GAP

To conclude, my mission is focused on making security optional not making security obsolete. Because making security obsolete says “just listen to me, let me take care of it and you can count on me to do something”. Instead, I say my job is to empower you with information, and actionable intelligence that is designed to know the audience – know what is a concern to them and be mindful of all tools, technologies, and modalities in how I can connect it to benefit of my audience. And this simple change has not only been critical for the effectiveness of my programme but developed a sustainable defence mechanism to strengthen the best security that money can buy – **Human Intelligence**. Period!

In the current information age, Security and Privacy awareness training programme need to incorporate so much more than organisational policy and compliance checkbox deliverables. So, defy the status quo and be convicted to help your audience to protect them and their wellbeing. Business security posture, resilience and compliance will be a by-product.

CONTACT US

UK OFFICE
20 - 22 Wenlock Road, London
N1 7GU, UK
Company Number - 12949110
UK ICO Registration Number -
ZB024341

NEPAL OFFICE
Stupa Infosec Pvt. Ltd.
Bansidhar Marga, Chandol
Kathmandu, Municipality,
Nepal

www.stupa.io
info@stupa.io

Meritec Ltd.
Acorn Business Park, Skipton
North Yorkshire
BD23 2UE

www.meritec.co.uk
digitallearning@meritec.co.uk

Our Cyber Awarness e-Learning Course -
Simple to understand and easy to consume

Scan here to learn more

Stupa Ltd

Meritec Ltd

MERITEC
Talent & Technology

stupa
VISION BEYOND PROTECTION