

TABLETOP EXERCISES



SIMULATE, EXERCISE &
COLLABORATE



INTRO

How do you motivate and engage your employees to care about cybersecurity and mitigate social engineering attacks?

Meet John! John has been a CISO of Y-Company for five years now. Ever since COVID-2019 disrupted ways of working in his organization, he has had some sleepless nights. Cyber-attacks have seen a sharp rise of 600%, and over 75% are because of human error.

Despite all the cybersecurity awareness and training, no one seems to care! Only 45% of the entire workforce is taking these training sessions. And half of them keep making the same mistakes. His management and peers understand that cybersecurity is critical; it keeps popping up everywhere. And yet, cyber breaches keep taking their toll on him and his team.

We helped John turn this around. We worked with John and his peers to design and facilitate Tabletop Exercises where Stakeholders, Senior Leadership, Management Teams and Staff exercise collaborative leadership.

“

600% CYBER
CRIME INCREASE
SINCE COVID-2019
BEGAN

They leave with a toolbox on how to fuel IQ & EQ simultaneously, increase stress tolerance, build resilience, engage stakeholders and build thriving teams. The TTE replicates cyber attacks based on social engineering techniques to inflict cyber crime such as the most prevalent phishing attacks, ransomware attacks, impersonation and identity theft.

Lisa, a marketing manager with the company, loves this approach! She has been struggling in managing her team remotely and handling all the increasing workload. Now, not only has she learned how to foster cyber hygiene, preparedness and resilience within her team: she also has a toolbox to increase her team's productivity and engagement levels despite disruptive external factors.

Within six months, the participation rate in this training has gone up to 85%. The human error went down from 75% to 44% as people learned how to build their emotional firewalls and filter phishing attacks, the most prevalent social engineering attack.





Do you lay awake at night worrying about a potential cyber attack? Or do you worry about how to recover and prevent the next one?

Every organization knows deep down that if they have not been attacked yet; they will be at some point.

At NATO, preparedness was at the heart of our core business. If we were not in conflict, we were exercising our ability to be prepared for the unknown and the next disaster.

What if your stakeholders, your leadership, your management teams, and your employees knew what to do and how to do it when a cyber-attack occurs?

At NATO, we focused rehearsing response options in future scenarios helped us push the collaborative comfort zone and moved us from complacency to empowerment.

We learned to become comfortable with the unknown and threats as we continued to build preparedness for the next crisis.

This is the same principle we apply at our Tabletop Exercises at Thrive with EQ.

Our objectives are to :

- Build functional trust between diverse and multi-disciplinary teams
- Clarify roles and responsibilities and exercise implementing plans of actions during simulated cyber threats.
- Identify your bottlenecks, challenges, and obstacles in addressing the human factor of cybersecurity.
- ...provide you with an unforgettable team-building experience.

Our lives and digital footprint do not have to be hijacked by cyber criminals.

Instead we can take back control by applying our full human potential in the digital age.

Are you ready to stimulate, exercise, and collaborate in preparing your (remote) teams to beat cybercriminals at their own game?

What are Tabletop Exercises (TTEs)?

Tabletop exercises are interactive, engaging, and dynamic sessions to help you clarify roles & responsibilities, improve problem-solving and decision-making, and enhance collaboration during cyber attacks. Thrive with EQ focuses on helping you engage and lead your teams during times of disruption and high-stress environments.

What makes your TTEs unique?

One of the greatest misconceptions about cyber is that it is purely Information Technology related. With an increase of 600% in cybercrime since COVID-2019 began, of which 96% are based on manipulation of human vulnerabilities, and with over 78% of remote workers worldwide costing the global economy an estimated 1 Trillion USD in 2020. We focus on exercising all the non-IT elements of a cyber attack and help you build cyber preparedness and resilience through collaborative leadership.

What do you exercising during TTEs?

Our TTEs are designed based on the specific client's desired outcomes and requirements to ensure the simulations provide a realistic experience. During the cyber crisis simulations, and as agreed with the client, we offer various collaborative leadership modules, which you can view here. We use a dedicated Microsoft SharePoint client portal with secure cloud-based solutions and advanced cyber threat protection.

How do you deliver the TTEs?

Thrive with EQ's TTEs can be organized both in a virtual environment or in person. The client can choose the desired platform – we deliver online TTEs on Microsoft Teams, Cisco Webex Training, or Zoom. Every TTE includes a Microsoft client SharePoint portal, which covers the full information management life cycle of collaboration with our clients.





TTE OBJECTIVES

- Understand the basics of social engineering attacks and the correlation with emotional intelligence, human vulnerability and remote productivity.
- Exercise collaborative leadership focused on fuelling your IQ & EQ, increasing stress tolerance, building resilience, engaging stakeholders, communicating during crisis and building thriving teams.
- Implement a dual-track approach to increase cyber hygiene and people's potential in navigating cyber threats in the new ways of working.
- Simulate real-life inspired cyber crime scenarios and incentivize new behaviours in mitigating the impact of social engineering attacks.
- Empower your ecosystem of stakeholders, customers, and employees to become part of the solution and embrace a new cyber preparedness culture for the hybrid or completely remote working environment.
- Exercise building and sustaining trust with your customers, stakeholders and employees.

COLLABORATIVE ENGAGEMENT



FUEL YOUR IQ & EQ



INCREASE STRESS TOLERANCE



BUILD RESILIENCE



ENGAGE YOUR STAKEHOLDERS



CRISIS COMMUNICATIONS



BUILD THRIVING TEAMS



APPROACH

STEP ONE

Let's get to know each other and connect over a virtual business chat. We want to listen to your challenges, your requirements and desired outcomes for a mature cyber preparedness strategy.

STEP TWO

Once we had an initial chat, we will schedule your DEMO session of our secure client portal. We will walk you through our comprehensive tabletop exercise with sample scenarios and collaborative engagement exercises.

STEP THREE

If you feel convinced of the value-added of our TTEs, we will send you a tailored value proposition for your consideration. It will include our solutions for your specific problems discussed beforehand with several options you can choose from.

STEP FOUR

Once you decide to accept our value proposition, we can get started immediately. Our clients have full visibility and can choose the level of collaboration during the entire process. You will have secure access and overview to our cloud-based client portal at all times.

[**BOOK MY VIRTUAL BUSINESS CHAT**](#)

TESTIMONIALS

World Savings Banking Institute (WSBI) and Global Cyber Alliance joined forces and organized a series of webinars on “Cyber Transformation: From Strategy to Operations”. Thrive with EQ led the regional training webinars for our members in Latin America, Africa, Asia and Central Europe. The CEO, Nadja El Fertasi, facilitated transformative, innovative and dynamic online training which focused on exercising collaboration during a simulated cyber crisis. Our members learned new ways of approaching stress management, problem-solving, decision making while navigating a disruptive cyber event. Nadja’s work ethic while looking for excellence, coupled with a good sense of humor, enabled us to approach our customer needs best, while working in flexible and convivial manner. I certainly recommend Thrive with EQ’s Table Top Exercises for any organization who is looking to exercise collaboration and be prepared against the inevitable cyber disruptions of the digital age.

Laurie Dufays, Head of Institutional Relations with Africa at WSBI-ESBG

I have known Nadja since October 2016 and she is one of the most passionate, creative, intelligent and ambitious individuals I have met. Her global vision and leadership in driving change is an inspiration for all who work with her.

Denis Mercier, Deputy General Manager at FIVES Group and former Supreme Allied Commander for Transformation at NATO, September 2019 (2015 - 2018)

I had the pleasure of participating in the inaugural cyber crisis simulation exercise at the GLOBSEC 2019 Bratislava Forum on 6 June 2019. Nadja designed two out of the four innovative, strategic and real-life cybersecurity scenarios. I participated in one of them and found the emotional intelligence aspects to be critical for decision-making and problem solving within diverse teams and under high pressure. I have known Nadja for several years now and she continues to impress me with her creativity and leadership.

Benedetta Berti, Head, Policy Planning, Office of the Secretary General at NATO

She designed and facilitated a real-life cybersecurity scenario with five uniquely designed personality types across generations, cultures, backgrounds, and sectors. The role-play allowed us to step outside our own map of the world, develop more empathy for other team members, develop greater self-awareness and become more rational decision-makers and problem solvers.

Muddassar Ahmed, Managing Partner at Unitas Communications, Founder & President of John Adams Society, Founder & Chair of Concordia Forum, Advisory Board Atlantic Council



ABOUT THE CEO/FOUNDER

For nearly two decades, Nadja has worked at NATO, the world's largest crisis management organization. Her last position was Senior Executive at the NATO Communications and Information Agency, responsible for strategic stakeholder engagement and communications for implementing NATO and Nation's Digital Transformation programs.

Having worked closely with people from over 40 countries, she is uniquely skilled in fostering trust and understanding among diverse, global stakeholders in both the public and private sectors across various industries.

At Thrive with EQ, Nadja designs and facilitates cyber-crime simulations to help people build emotional firewalls against social engineering attacks. She addresses the human factor by exercising collaborative leadership skills during cyber crises. Nadja possesses the latest credentials in the field of emotional intelligence and trained with leading experts in the field.

Nadja's character is what defines her passion and purpose in her work and the relationships with her clients. Her personality is fuelled through her character signature strengths, which include creativity, wisdom, humor, bravery, social intelligence, curiosity and kindness. She is fluent in Dutch, Arabic, English, French and has a good understanding of Italian and German.

[DOWNLOAD HER BIO](#)

LET'S CONNECT

Nadja El Fertasi

CEO/Founder
Thrive with EQ



<https://thrivewitheq.com>



info@thrivewitheq.com



+32(0) 471907005