KEPNERandFOURIE™
Critical Thinking Technologies

Thinking DIMENSIONS GLOBAL

*Self*CYBER™ Cyber Solutions Expert Program

Arm yourself by protecting the 20% that's providing the 80% opportunity!

Only when you apply your best thinking and resources to the cybersecurity challenge will you be able to sleep at night Matt Fourie - KEPNERandFOURIE

The power of INTERNAL SPECIALISTS continually addressing pro-active and reactive cybersecurity issues

Nobody wants security breaches and the only way you will be able to keep the threat actors out will be your level of attention given to this challenge. In more than 80% of hacking cases the vulnerability areas affected were not even anticipated and was a complete surprise to the internal Risk Team. This situation makes it imperative to have internal teams continually assessing potential threats at all times and continually improving the stability of hardware/software applications. This approach will provide well-articulated quality data and the means for having meaningful interdepartmental interactions at the Risk Forum meetings.

Imagine having highly trained and "experienced" in-house experts on-staff that could lead the initiative ensuring they meet the threat actors' heads-on? We provide an intensive "development program" equipping well-chosen in-house IT Professionals deployed in a very specific way to be the "firewall" between threat actors and company critical systems.

WHO SHOULD DRIVE THIS?

The secret to success is the presence of well-trained internal "Security Solutions Experts" (SSEs) deployed inside the organization. The following roles are critical:

- **Cybersecurity Core Team** – A team of strategically chosen staff members to overlook and oversee all efforts to improve internal security practices.
- **Master Cyber Solutions Expert (MCSE)** – A well trained CHAMPION coached by Thinking Dimensions in a full time position to continually lead Continual Security Improvements. **Cyber Solutions Practitioners** – Additionally trained and developed in-house experts assisting the MCSE on a part time basis to help with facilitating cyber solutions.
-

PROCESSES

The following thinking approaches will be covered:

1. **Threat Assessment**
   - **Cybersecurity HeatMap** – Identify the 20% processes with an 80% breach potential
   - **Process Continuity Analysis** – Identify all vulnerabilities in any co process.
   - **Solution Strategy** – Determine the most effective Cyber Solutions strategy

2. **Solution Development**
   - **Breach Mitigation Analysis** – Determine likely causes of breaches to generate protection.
   - **Threat Solution Design – Max4 Solutions** – Design solutions to ensure business continuity.
   - **Human Error Screen** – Screening presence of typical human factors causing breaches.

3. **Fixing Breaches**
   - **Breach Incident Analysis** – Ability to address breaches quickly and accurately.
   - **Breach Problem Analysis** – Identify both Technical/Root causes enabling permanent fixes
   - **Human Error Realignment** - Correcting company related issues causing "human error"

AN EXCLUSIVE ACCREDITATION

Thinking Dimensions in partnership with the Loyalist Examination Services (LES) and The Institute for Professional Problem Solvers (IPPS) is offering the following professional certifications when the incumbent has successfully completed their Cybersecurity development:

- **Foundation certificate** when they completed the 1ST block of 3 days successfully
- **Practitioner certificate** when the incumbent completed the additional block of 3 days successfully – **Cyber Solutions Practitioner**
- **Master certificate** when the incumbents have managed a completed Continual Security Improvement initiative successfully. This is the ultimate accreditation of **Cyber Solutions Master**

WHY AN IN-HOUSE APPROACH?

"Leverage resident intelligence to combat cybersecurity threats!" This is true, because nobody knows your critical systems better than your own staff.

- In-house specialists will always have their ears on the ground and will assess and fix potential threats on an ongoing basis.
- Having your own "in-house consultant" will make you self-reliant and the best approach to combat security threats
- Your internal experts will develop your own unique repeatable model with company unique and modified tools and techniques for ongoing use in the future.
- This changes the traditional "top-down" approach to a full ownership "bottom-up" approach; improving buy-in and commitment for RiskTeam suggested fixes.

TOP 5 REASONS TO ATTEND

- The use of the world renowned KEPNERandFOURIE problem solving approaches to provide a sound grounding for the collective thinking of your own staff.
- Thinking Dimensions is "transferring" all their "know-how" to you as their client with continual support from TD when needed.
- Develop your own approach through organic learning, which will be working well for your unique security proofing needs.
- *Self*CYBER™ is focusing on the processes surrounding the "interaction" between Humans and Technology, which we believe is posing the greatest threat for breaches.
- Lastly, you will develop a new habit of repeatedly assessing and fixing all critical operations for potential threats in what we call "Continual Security Improvement" practices.

CONTACT US

For more information, please contact our Local Malaysian Representative:

KEPNERandFOURIE Thinking Technologies traces its origins back to 1997. It was then that Dr. Chuck Kepner and Dr. Matt Fourie collaborated on the design and delivery of problem solving and decision making techniques to some of the leading companies of the world. Companies that required – better, faster, and more flexible techniques to improve performance significantly.