KEPNERandFOURIE™
Critical Thinking Technologies

Thinking DIMENSIONS GLOBAL

*Self*CYBER™ Foundation Workshop

Be self-armed in all aspects of how to protect our assets!

"Your best ally in fighting cyber crime is your own staff!"
-Matt Fourie - KEPNERandFOURIE

The power of collective pro-active cybersecurity thinking that will make your efforts in cyberproofing worth it

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. Vulnerabilities are evolving all the time and this makes it critical "to have eyes on" all your existing and potential vulnerabilities. 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 constant efforts being employed to fight all real and imagined security threats and risks.

It is all about empowering local resources at source to fight cyber crime on a daily basis. This attitude will ensure excellent buy-in by managers and staff in helping their own organization and ultimately themselves to stay safe and secure. The simple fact is that if staff do not understand and buy-in to this thinking your company will have a major potential problem dealing with cyber attacks on an ongoing basis.

WHO SHOULD ATTEND?

This workshop is primarily for all company staff directly and indirectly involved in company IT practices and processes. The following would be priority target groups:

- **All Managers** – Managers need to understand the existing and potential threats of all staff actions that could cause or allow cyber attacks.
- **Company Risk Officials** – Any risk officer that is responsible for some part of the company's risk practices.
- **Key Employees** – Any key employee working with sensitive technology (hardware & software) and/or processes around these technologies.

PROCESSES

The following tools and templates will be covered:

1. **Threat Assessment**
   - **Cybersecurity HeatMap –** Identify the 20% processes with an 80% breach potential. Will identify "hot spots" and processes with particular risk vulnerabilities.
   - **Process Continuity Analysis –** Identify all threats & risks in any company process or practice. These would include technology and social vulnerabilities.
   - **Potential Threat Analysis –** An advanced focus on specific treats associated with either a technology, company process or "human error" issue.
   - **Solution Strategy –** Determine the most effective Cyber Solutions strategy to reduce the probability of certain threats and risks occurring.

2. **Solution Development**
   - **Breach Mitigation Analysis –** Determine likely causes of breaches, threats and risks to generate protective and mitigation actions to reduce the probability of these threats.
   - **Threat Solution Design – Max4 Solutions –** Design solutions to ensure business continuity. These solutions will be designed with internal cost effective and doable actions. When combined these actions would form a major effective "barrier" for possible threats.
   - **Human Error Screen –** Screening presence of typical human factors causing breaches. These factors are normally Management and company specific issues to be corrected.

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.

- Staff will always have their ears on the ground and will be a major contributing factor in fighting security risks.
- In-house training could be customized to address company specific challenges more effectively during the actual workshop time.
- An in-house option provides for more effective & meaningful personal learning experience.
- Workshop could be delivered in a daily permutation that would ensure the least disruption to existing work practices and workload.
- This will change a poor supported "push" approach to a well supported "pull" approach with exponentially improved data.

TOP 5 REASONS TO ATTEND

1. The use of the world renowned KEPNERandFOURIE problem solving approaches to provide a sound grounding for the collective thinking of your own staff.
2. Thinking Dimensions is "transferring" all their "know-how" to you as their client with continual support from TD when needed.
3. Develop your own approach through organic learning, which will be working well for your unique security proofing needs.
4. *Self*CYBER™ is focusing on the processes surrounding the "interaction" between Humans and Technology, which we believe is posing the greatest threat for breaches.
5. 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:

Bill Dunn USA East Coast billdunn@thinkingdimensions.com
Robin Borough USA West Coast robin@thinkingdimensionsassociation.com
John Hudson United Kingdom john@thinkingdimensions.com
Adriaan du Plessis Africa adriaan@thinkingdimensions.co.za
Andrew Slauter ANZ andrew@thinkingdimensions.com.au
Steven Loo APAC sloo@thinkingdimensions.com.sg
Matthys Fourie Global mat-thys@thinkingdimensions.com
Jay Jayshankar India jay@thinkingdimensions.com

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.