KEPNERandFOURIE™
Critical Thinking Technologies

Thinking DIMENSIONS GLOBAL

*Self*CYBER™ Cybersecurity Fact Sheet

A Facilitator workshop to develop In-House specialists as Cybersecurity Solution Experts (CSEs) impacting security practices on a daily basis.

OVERVIEW

This program will equip the participants to utilize the various KEPNERandFOURIE™ Investigation processes to bring about proactive and reactive excellence in managing Cybersecurity issues. Security breaches are a reality of everyday life. The only way you will be able to keep the threat actors out will be to ensure your staff have the adequate investigative skills to address this issue. 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 an internal team assessing potential threats at all times and continually improving the stability of hardware/software applications and their interaction with business processes and staff manning those processes.

THINKING SKILLS

The ability to apply in-depth Security Proofing resolution-thinking processes to any pro-active and reactive security problem situation will address this concern.

What it is

Problem solving skills that are systematic, systemic, intuitive and logical. This will help the individual or team to address each problem situation correctly, swiftly and effectively.

What the participant will learn

- How to assess and diagnose potential security vulnerabilities.
- How to harness the collective thinking of staff at source to generate and execute highly effective self-empowered security proofing strategies.
- How to create and/or develop cybersecurity solutions using the most effective process, tools and templates as the input vehicles for desired outputs.
- How to develop the internal skills and processes to deal with security breaches quickly and effectively.

IN-HOUSE FACILITATION

Providing the knowledge and skills on how to assist others in the organization in their cybersecurity problem solving and decision making efforts.

What it is

The ability to lead and manage an executive team, taskforce, project team or workgroup to work through a specific security problem to achieve a specific result.

What you will learn

- The ability to use the appropriate cybersecurity problem solving tools to diagnose a cybersecurity situation and then to facilitate the solution nominating the correct information sources and process to be used.
- The ability to facilitate and manage group inputs, especially in difficult and sensitive situations.
- The use of interrogative questioning techniques to generate the correct information.
- The ability to manage and organize data visually and logically in order for the participants to more effectively analyze them. -
- The ability to adapt to a security threat or breach situation in such a way that speedy results are achieved.
- The ability to merge problem solving processes with other continuous improvement initiatives, such as Six Sigma and LEAN Enterprise.

PROCESSES

The following tools and templates will be covered:

To equip the participant with the ability to use the KEPNERandFOURIE™ processes, tools and templates in such a way that will foster high levels of buy-in, commitment and successful implementation of strategies.

Workshop Materials

The workshop provides the participants with the ability to apply all the tools and templates in any configuration to fit the security concern.

Tools and Templates

The following are the tools and templates of the complete suite of Cybersecurity applications. These tools constitute the major part of the CSE development program.

1. **Threat Assessment**
   - **Cybersecurity HeatMap** – To identify the 20% company practices/ processes with an 80% breach potential
   - **Social Engineering Assessment** – To determine the company performance processes factors which constitute potential root cause elements of security breaches.
   - **Human Error Analysis** – To determine if there are any potential weak human performance elements present in exiting IT practices and processes.
   - **Process Continuity Analysis** – To identify all the potential "weak and blind spots" in an IT process that could be subject to a breach.
   - **Threat Re-Focus Analysis** – To identify the core issues represented in a potential threat in order to make the generation of corrective actions more focused and more effective.
   - **Solution Strategy** – To determine the most effective solutions strategy to minimize actual breaches and discourage internal and external threat actors

2. **Solution Development**
   - **Breach Mitigation Analysis** – Determine the likely causes of a breach to generate preventive/contingent actions in order to mitigate the probability of a breach occurring.
   - **Threat Solution Design** – Develop designs and solutions to ensure business continuity using various solution and design models as well as innovation techniques.
   - **Human Error Screen** – Screening ten (10) human error factors that could be present in an existing IT practice, which unless addressed, could cause an opening for a breach.

3. **Breach Restoration**
   - **Incident Management Analysis** – To help a team to develop the ability to address a breach incident quickly, accurately and permanently.
   - **Problem Management Analysis** – To launch a special investigation to identify both the technical cause and root cause of a security breach to enable a permanent fix.
   - **Root Cause Analysis** – To instill a mindset of looking for underlying reasons before trying to fix anything. The aim is to steer staff away from trying to fix effects and rather focus them on fixing causes.
   - **Human Error Realignment** - To use the correct tools and techniques when specific human behaviors are involved in a breach.

The FOUR PHASES of the KEPNERandFOURIE™ Cybersecurity *Self*CYBER™ Approach

1 ASSESSMENT
Learning how to use the Cybersecurity tools and templates
- **Cyber HeatMap**
- **Process Analysis**
- **Threat Analysis**

2 DISCOVERY
Do an own-job investigation for use in the 2nd week of application
- **Identify a Process Owner**
- **Gather Info**
- **Confirm Project**

3 APPLICATION
Use process owner background for all Cybersecurity applications
- **Mitigation Analysis**
- **Solution Design**
- **Human Error Screen**

4 COACHING
Using the newly developed Cyber Solution Experts (CSEs) for live initiatives
- **Use Tools**
- **Assessment**
- **Facilitate Solutions**

IMPLEMENTATION

To SUPPORT a Continuous Service Improvement (CSI) Cybersecurity culture that will ensure all the key employees at all levels in the organization are effectively positioned to provide timely diagnostic intelligence and suggest appropriate solutions.

What it is

Training in-house Cyber Solutions Experts in problem solving facilitation to enable them to facilitate and/or coach company employees in the ongoing effort to instill proactive and reactive security thinking and skills.

Why an In-House Approach

"Leverage resident intelligence to combat cybersecurity threats!" This is true, because there is no one who knows your critical systems better than your own staff.

- In-house specialists will always have their ears to the ground and will assess and fix potential threats on an ongoing basis.
- In-house specialist facilitators will be available to any manager at the drop of a hat to assist in any investigation. They are also available to provide advice.
- Having your own "in-house consultant" will make you self-reliant and is the best approach to combat security threats
- Your internal experts will develop your own unique repeatable model with company specific and modified tools and techniques for ongoing use.

Inside a Typical Initiative

Thinking Dimensions is not attempting to train or educate any key staff in cybersecurity. The objective is to develop in-house expert facilitators that will serve as in-house consultants addressing and fixing cybersecurity issues. The initiative will typically be implemented in the following phases:

- Start with Risk Management expressing the desire to become highly effective in addressing cybersecurity issues with internal experts and not to be solely dependent on consultants. Management will scope the length and breadth of the initiative including objectives and metrics to be achieved.
- Thinking Dimensions will then provide Cyber Solution Expert (CSE) selection guidelines for a minimum of four (4) CSEs to be developed. The total development time per CSE is nine (9) days. See that timeline/schedule above/below:
- CSEs start their development:
  - **a) Assessment**: First Development Phase (3-days) – CSEs learn and apply all SelfCYBER™ tools, templates and techniques.
  - **b) Discovery**: TD Consultant and CSEs conduct the initial "Cybersecurity HeatMap" to identify the 20% practices/processes that could be addressed.
  - **c) Application**: Second Development Phase (3-days) - CSEs to practice with feedback and coaching on "live" issues.
  - **d) Coaching**: Third Development Phase - CSE further their development through on the job coaching and feedback working through a whole life cycle of cybersecurity issues.
- Once this CSE development cycle is completed, Thinking Dimensions will make a recommendation as to which CSE would be the best candidate for the full time CSE allocation; the rest will be part-time in-house facilitators.
- All CSEs will received their official accreditation and certificates from Loyalist Examination Services on behalf of the Institute for Professional Problem Solvers (IPPS).
- After the completion of the 1st round sessions and implementation of fixes TD and Client will assess the rate of successes achieved and will then generate action steps to "correct" any misaligned practices.

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**

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.

CONTACT US

For more information, please contact:

Lead Consultant:
Matt Fourie: mat-thys@thinkingdimensions.com
Support Consultants:
Bill Dunn: USA: East Coast
billdunn@thinkingdimensions.com
Robin Borough: USA West Coast
robin@thinkingdimensionsassociation.com
Andrew Sauter: ANZ
Andrew@thinkingdimensions.com.au
John Hudson: UK & Europe
john@thinkingdimensions.com
Steven Loo: Asia & Singapore
sloo@thinkingdimensions.com.sg
Jay Jayshankar: India
jay@thinkingdimensions.com.in
Juan Fourie: USA
jcfourie@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.

Thinking DIMENSIONS GLOBAL

KEPNERandFOURIE™ Critical Thinking Technologies