Q1 2014
ISSN 2046-5874 (Online)

Continuity

The Magazine of the Business Continuity Institute

20 Years of the BCI

WHAT LIES OUT THERE?
Findings of Horizon Scan 2014

READY TO RESPOND
The UN's approach to BCM

MAKING THE DISTINCTION
Moving from incident to crisis

Mega-trends reshaping BCM

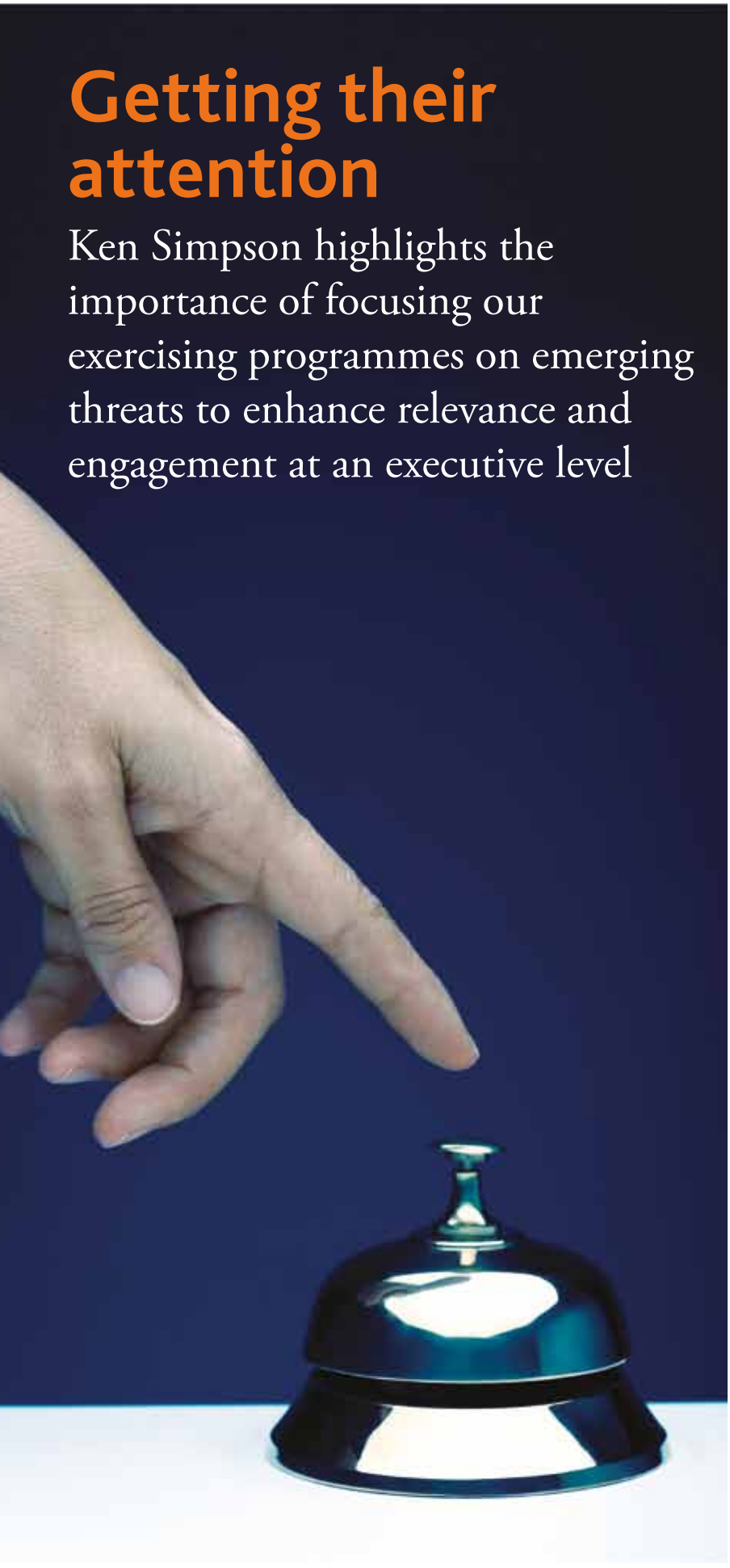
A fundamental change in approach to continuity

Business Continuity Institute

Visit the BCI website www.thebci.org

Getting their attention

Ken Simpson highlights the importance of focusing our exercising programmes on emerging threats to enhance relevance and engagement at an executive level



Have you ever found yourself in a situation like this? You have designed and delivered a BC exercise that was well constructed and technically sound, supported your objectives for a multi-year exercise programme, and included a good debrief allowing you to capture a number of improvements for your plans. Despite this, however, the executive team either stayed away, or didn't engage and were on their iPhones/Blackberries throughout the activity.

If you have, then read on as this article may help.

Executive engagement

Technical excellence in designing and running an exercise is not enough to generate executive engagement. Your content and the way the exercise is conducted are critical.

The biggest obstacle to engagement encountered by many BC practitioners is that the programmes they operate are focused on fighting the last war, rather than aiming to develop the skills and capabilities required for future conflicts. You can recognise these battles of 'BCM-past' by their focus on operational issues, often using incidents that do not warrant being described as a crisis, or demanding executive attention. They are missing the point on the exercise content.

Another noticeable feature of these activities is their focus on exercising documented plans and procedures. The exercises are conducted in a way that fails to meet the needs of executives.

Generally, this occurs because they fail to understand that executives are not procedure followers, they are problem solvers. If you want to get their engagement then you need to exercise their minds rather than your documents. The focus must be more on the crisis aspects and less on the procedural recovery tasks.

Holding their attention

One way to freshen up your exercises, and generate greater executive engagement, is to explore the impacts that can arise from emerging risks. These scenarios can cover a range of threats that are generally not widely understood, nor the subject of detailed plans. Exercising the response to such a threat will require not only problem solving, but also fresh thinking and fresh practice in the BCM area.

Part of this fresh thinking and practice is understanding that you need different scenarios, impacts and formats (and perhaps different exercises) to meet the needs of different stakeholders, including strategic executives, senior tactical managers, operational and logistical functional areas.

For executives you need to assess your exercises in terms of their relevance:

- Is the content relevant to the executive? Do you understand their needs?
- Will the way the exercise is conducted enable the executive to develop trust in the organisational response?
- Will it be relevant to how they perceive they will run a real crisis response? Otherwise they will not want to attend the next exercise.

We address relevance when what we offer overlaps with what the other party needs. For executive exercises that means scenarios that are on their risk horizon – and at a level of impact where they operate.

The World Economic Forum (WEF) publishes an annual Global Risks Report and the 2014 edition[1]

©iStockphoto.com/lorrainedarke

highlights the need to explore and understand interdependency. A simulation exercise can be very effective for this purpose. The top global risk for 2014 is "fiscal crises in key economies" – not fire, burst pipe or server outage.

Fresh practice includes widening our focus of threats. Liquidity problems are not a new or emerging threat, but they can contribute to this emerging area of attention. If you are a BC practitioner in financial services and you cannot, or have not, pulled together a liquidity-related exercise then you may have a relevance problem. I addressed this issue of relevance in more detail in a previous article entitled "Putting management into BCM"[2].

The cyber threat

Over the last nine years, I have had success engaging executives in exercises that explored cyber threats. Cyber was not the only scenario used in that period, but the engagement has often been more pronounced when emerging threats such as a cyber-related incident are employed.

One of the best examples of this came from a recent exercise in New Zealand where participants described it as "more challenging than responding to the Christchurch earthquake". The challenge arose from their limited understanding of the nature of the threat and the different continuity responses that were required for a non-physical event.

Cyber threat is an effective place to start exploring emerging risks. Today it is widely acknowledged as a threat[3] and also exhibits the attributes of emergence as it changes and evolves as the systems and attackers interact with each other. This scenario can be used to generate the unexpected interdependence and systemic impacts that the WEF Global Risks Report is concerned about.

> "The challenge arose from their limited understanding of the nature of the threat and the different continuity responses that were required for a non-physical event"

Here are some key learnings that you might want to take into account when you consider using a cyber-related threat to engage your executives:

- The BC team cannot do this without the close co-operation of the IT leadership and the IT security team.

  This is a feature of all emerging risks, they require a multi-disciplinary team to collaborate to understand the problem and design the exercise.

  Don't be surprised if your IT executives are not able to articulate the cyber threat to their business peers – it will be new to many of them also. This is not the place to pressure or ambush them, it can also be a rehearsal for them – conscript and work with them as part of your exercise delivery team. You need to script their response to reflect actual activity and to manage the flow of the exercise.
- Despite the need for IT engagement, do not try to engage your executives with a detailed IT technical response exercise. Again the collaboration is about taking the technical impact and translating into business impacts – this should be a core competence of the BC discipline. Remember that cyber threat is not an IT problem – it is a whole of business issue to address.

- Avoid the simple variants such as a basic PC virus or a Denial of Service attack. These tend to deal with the availability of your systems in much the same way as a server failure does – they also tend to be very operational.

  Consider more sophisticated attacks that can damage the integrity of the data in your systems, or breach confidentiality.

  Also consider cases such as the recent data breach at US retailer Target that compromised the data of 70 million customers. This type of scenario relates to an intrusion that started in the past – the extent of the loss/damage is often unclear in the short-term.
- Work with your IT colleagues to understand what else is connected and exposed to a cyber threat. For example:
  - > IP Telephony can put your ability to communicate in the crisis at risk.
  - > Customer-facing (web) systems, impacting sales and brand.
  - > SCADA devices that control power, engineering and elevators are increasingly connected to IP network.
- Cyber threats can focus attention on a single company rather than wide-area physical disasters. This provides the heightened media/regulatory scrutiny that is needed for executive engagement.
- Encourage your IT team to exercise the same scenario at the operational level – capture the executive requirements as input to this exercise.

A new understanding

When dealing with emerging risks we need to clearly understand that best practice can be past practice. These practices may not be applicable or effective in dealing with new threats and risks. The exercises may become the vehicle to understand the risk and the potential response – any documenting of plans and procedures would come later.

We have to be prepared to experiment with fresh or novel practices to address new risks and threats that we do not fully understand. These practices may require a truly collaborative approach with other disciplines in the organisation and embrace a wider category of risks than are considered in the scope of BCM.

(Endnotes)

1 *http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf*

2 *Business Continuity and Resiliency Journal, Quarter 3, 2012, also a webinar https://www.brighttalk.com/webcast/6059/59493*

3 *There is even an international conference on Cyber Crisis Exercises – http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/conference/2nd-enisa-conference*

KEN SIMPSON MBCI

Ken Simpson, director, The VR Group Pty Ltd

Ken@VRG.net.au
www.blog.vrg.net.au
www.vrg.net.au

©iStockphoto.com/lorrainedarke