Yes! And
Think Innovatively

Is your whole business ready to deal with a cyber attack?

In a highly publicised cyber attack in the UK, criminals stole the bank account details of thousands of customers from a company. One consequence was that the shares of that company lost a third of their value; they estimated the cost to resolve the situation at £35 million and the reputational damage is yet to be assessed.

This is just one of many instances where companies have suffered financial, reputational and / or Intellectual Property (IP) loss through cyber crime. We are sure that all of these companies were satisfied with the risks they faced and the measures employed to protect their data. Yet, the worst happened. Their security was breached.

Could this happen to your company?

Do you know:

- All of the cyber security threats to your company's Communication and Information Systems (CIS)?
- All the business risks and impact associated with a breach of CIS security and data loss?
- What data is essential and valuable to your business and so a potential target for thieves?
- Your company's plans and response and the responsibilities of each person in the leadership team, in the event of a cyber security attack?
- If you could justify your plans or response to the Board or shareholders?

If your answer is:

- **NO**, to any of these questions, is it time to take action?
- **YES**, to all of these questions, do your leadership team colleagues and / or Board have a similar level of knowledge? Will they be able / willing to provide the correct level of support if a crisis hits?

Formulating a response

Cyber threats are not just a technical issue. They are an issue that the leadership team needs to deal with as a whole, with the help of relevant experts from the front and back office. The first step is to educate, formulate a high level response and initiate the first steps.

HOW MIGHT YOU DO THIS?

You could:

- Deliver training - but do you have the time for generic training solutions?
- Set up a working party - and have endless meetings that might not focus on critical business assets
- Bring in cyber consultants to provide a solution - but will they be truly independent, do they really know YOUR business, and what will your people learn from the experience?

An alternative:

A quick and effective alternative is to facilitate a meeting with the key people across your company who really understand the business and can identify the risks and the appropriate

responses. A meeting that will educate, encourage informed discussion and provide practical outputs. One that enables you to identify the risks, establish the first steps most appropriate to protect your business and assign responsibility for them.

Our Solution

In Yes! And, we provide a solution for this alternative. We design and facilitate an engaging and energised workshop to your exact needs, to help you:

- Create a non-technical understanding of the likely threats posed by cyber crime to your business

  Output – *a picture of the threats*

- Pinpoint the areas of your business most at risk, the level of that risk and the likely impact on different areas of the business.

  Output – *a risk register*

- Determine the responsibilities in event of a crisis.

  Output – *a high level response structure and plan with responsibilities*

- Agree the next steps to begin addressing the key issues.

  Output – *an immediate action plan.*

Why use us?

We have longstanding expertise in cyber and facilitating workshops. With no direct links to cyber security product and services companies, we provide an impartial and pragmatic approach to the issues. You can be certain that we focus only on the interests of your company.

Our Expertise

Jeff Parker – Cyber Expertise

Jeff is a former Vice President of Airbus Group with many years practical experience of working on systems associated with reducing cyber threats.

Jeff spent 23 years in the RAF working on communications, cryptography and computer systems employed in highly classified global networks. On leaving the RAF, Jeff spent 18 years working with Nortel and then Airbus working on strategy and business development for secure Communications and Information Systems (CIS) including Information Assurance (IA) and Cyber Security solutions. Jeff now uses his CIS, IA and Cyber Security knowledge to support organisations looking for innovative solutions to combat the growing cyber threat.

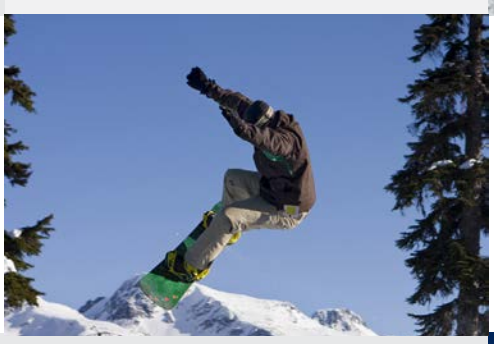
John Brooker – Workshop Facilitation Expertise

John is a former Senior Vice-President of Visa and since 2001, he has facilitated workshops with organisations such as Airbus Group, BT, Lloyds Bank, Roche, Unipart and Visa Inc. as well as medium sized companies. He helps senior teams to collaborate, engage and think in a more innovative way. He is particularly experienced with multinational and multicultural teams, having worked regularly throughout Europe, Middle East, Africa and Asia.

John was a tutor on the Open University MBA programme, "Creativity, Innovation and Change" for 14 years. He is a Board member of the Association for Solution Focused Consulting and Training and is the author of "Innovate to Learn, Don't Learn to Innovate," available on Amazon.

Next Steps

If you would like to explore our solution further, please contact us (see over for contact details). However, should you desire to learn more about our thinking and consider whether we are the right organisation to work with, please download a copy of our article here, or go to our website here http://www.yesand.eu/resolve-difficult-challenge/.



Yes! And
Think Innovatively

Contact Us

Write: hi@yesand.eu

Speak: +44 20 8869 9990

Read: www.yesand.eu