

# JAKOB SCHARF

**LONDON  
SPEAKER  
BUREAU**

- **Director General of the Danish Security and Intelligence Service (DSIS) from 2007-13**



*Jakob Scharf is former Director General of the Danish Security and Intelligence Service. During his term, he dealt with terrorism and cyber threats affecting national security interests and private corporations as well. Since he resigned in 2014 he is the executive director of CERTA Intelligence & Security, a consultancy company providing intelligence, analysis and security advice for private corporations.*

## Topics

- Cyber Security
- Risk
- Technology

### Masterclass overview

Technological development has created not only new opportunities but also new vulnerabilities and risks, including those of terrorism, political extremism, espionage, organized crime, cyber threats, and more. Today, security-related risks must be an integrated part of corporate risk management and focus must be on the ability of the corporation not only to identify, prevent and counter specific threats, but also to recover from specific incidents. In this masterclass devoted to strategic corporate security and risk management, Jakob Scharf works with your executive team to help you adapt your business to emerging global threats.

### Value and expected outcomes

- A unique insight into terrorism, political extremism, espionage, organized crime, cyber threats and other significant security threats relevant to private corporations
- Thorough understanding of the way private corporations need to adapt to emerging global threats
- A specific assessment of the maturity of your organization in dealing with security-related threats, risks and vulnerabilities

### What is covered?

Jakob Scharf will lead you through a series of discussions, which will enable you to answer the following questions:

- What are the most relevant and important security-related threats and risks affecting your organization?
- What are the consequences and how vulnerable is your organization in case of a security-related incident?
- Are the security level and security culture within your organization appropriate?
- Has your organization implemented such strategies, plans, guidelines and security measures, which are necessary and expected?
- Is your organization using its resources on security in the most cost-efficient manner?

