CYBER MANAGEMENT ALLIANCE

# Executive Briefings and Awareness Sessions

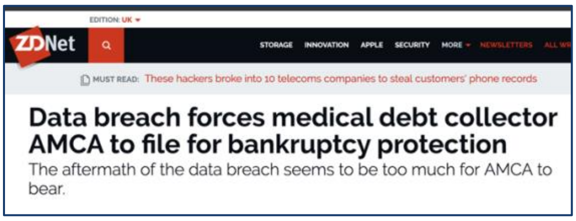
# Overview

## The Executive Briefing and Awareness Session

Given the facts, the business focus and taxonomy must shift from an IT and security narrative to that of resiliency.  The CEO, senior management and board must be asking if their business is prepared for and able to carry on business operations during and after a cyber crisis.  To survive and even grow your business, an organisation must put cyber resiliency at the heart of its cyber and digital strategy.

Cyber Management Alliance's Executive Briefing and Awareness Session (EBAS) is specially designed for executive management, CEOs and boards of directors, engaging them in a business context to help explain the threats and risks from cyber-attacks, and providing them with simple, tactical and strategic steps to help improve their resilience to reputation-damaging cyber crises.

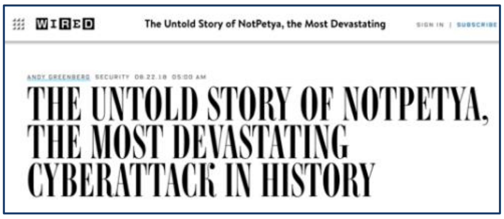
A cyber-crisis is often invisible and near impossible to detect in the early stages.  In many cyber-attacks, by the time a business detects the attack it is often too late.  The data has been stolen, the newspapers know about your attack, and your customers are worried about their personal data being in the hands of criminals.



MUST READ: These hackers broke into 10 telecoms companies to steal customers' phone records

Data breach forces medical debt collector AMCA to file for bankruptcy protection

The aftermath of the data breach seems to be too much for AMCA to bear.



The Untold Story of NotPetya, the Most Devastating

ANDY GREENBERG SECURITY 08.22.18 05:00 AM

THE UNTOLD STORY OF NOTPETYA, THE MOST DEVASTATING CYBERATTACK IN HISTORY

## Session Details

The Executive Briefing and Awareness Session is structured around key topics and based on our experience with clients from different sectors around the globe. However, it is flexible and can be tailored to the type of audience and business.

- The CEO and Board: we understand that time is a rare commodity for executives, like the CEO and board members. To that extent, the EBAS session lasts between 45 and 90 minutes.
- The Senior Executive: a typical EBAS session lasts between 2 and 3 hours, and includes one 15 minute break.

## **Preparation**:

In almost every situation we recommend at least one pre-workshop, 2-hour preparation session to ensure that we have a good understanding of the purpose, requirements and key outcomes of the session.

During this session, we also aim to understand the attendees, their vision and objectives, and the unique challenges the business is facing in the current environment.

**Target Audience**

| | |
|---|---|
| CEOs, Chairpersons | Business Unit/Division Heads |
| Legal Counsels | Directors/Heads of Sales & Marketing |
| HR Directors | CIOs & CTOs |
| Communications/PR Directors | Board members, Non-Executive Directors (NED) |

Where the session needs to be tailored to bespoke requirements, we will work with the client to ensure the session meets their requirements.

# Comparing our EBAS

| | Executive Briefing & Awareness Session | Other awareness sessions |
|---|---|---|
| Non-technical, business focused | Yes | Not always |
| Delivered by a leading cyber and privacy practitioner | Yes | Not always |
| Highly engaging delivery tailored to the type of audience | Yes | No |
| Focuses on the business and sector-relevant challenges | Yes | No |
| One-to-one, private sessions | Yes | No |
| Delivered globally, across various sectors | Yes | - |

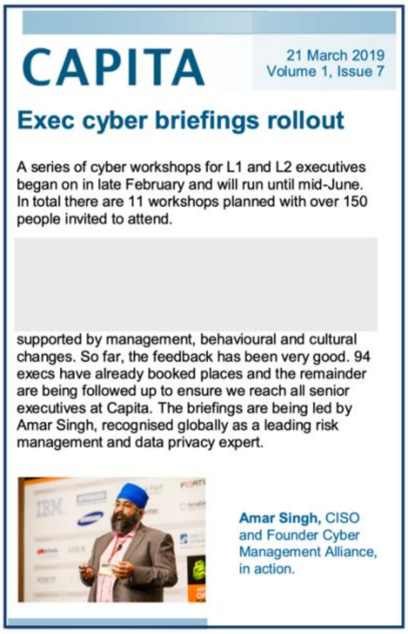
# EBAS - Workshop Structure

The Executive Briefing and Awareness Session structure is based on our experience with a broad range of clients from different sectors.  This can be customised as per your requirements.

| Time | Topic | Details |
|---|---|---|
| 10:00 | Introduction | • Introductions - why we are here<br>• Objectives and outcomes |
| 10:15 | Business Impact – Fact or Fiction | • Providing a pragmatic fact-based insight into the real and present threat from cyber-attacks<br>• Case studies – non-technical analysis of the business impact of attacks |
| 10:45 | **Threats & Risks**:<br>The Agents of Chaos | • Discuss the importance of threat actors, their motivation and the role of threat actors in scenario planning and risk management |
| 11:10 | **Threats & Risks**:<br>The Protection Fallacy | • Discuss and propose a better way than simply focusing on protect |
| 11:30 | **Threats & Risks**:<br>The Privileged User | • Insights and examples into the importance and relevance of privileges, and users with privileges |
| 12:00 | **Threats & Risks**:<br>The Golden Hour | • The relevance and significance of the Golden Hour and critical insights into what you can do to increase your chances of managing a crisis with little negative impact |
| 12:30 | What Would You Do? | • An interactive "What Would You Do?" session based on one or more attack scenarios |
| 12:45 | Takeaways & Recommendations | • A summary of what the business must focus on to improve its cyber resilience and overall maturity |
| 13:00 | Close  & FAQ | |

## Learning Objectives

- List key benefits of focusing on cyber resilience.
- Describe the simple steps and strategies a business can introduce to improve organisational cyber resilience, speed of detection and speed of response.
- Discuss the importance of privileges and credentials, and their role in maturing an organisation's cyber security and resiliency posture.
- Explain the business impact of cyber-attacks on under-prepared organisations.
- Discuss the importance of knowing about business-specific threat actors and their motives, and its importance in cyber risk management.
- Explain the importance of visibility and the key strategies to ensure an organisation is better prepared for the Golden Hour.



CAPITA

21 March 2019
Volume 1, Issue 7

### Exec cyber briefings rollout

A series of cyber workshops for L1 and L2 executives began on in late February and will run until mid-June. In total there are 11 workshops planned with over 150 people invited to attend.

supported by management, behavioural and cultural changes. So far, the feedback has been very good. 94 execs have already booked places and the remainder are being followed up to ensure we reach all senior executives at Capita. The briefings are being led by Amar Singh, recognised globally as a leading risk management and data privacy expert.

**Amar Singh**, CISO and Founder Cyber Management Alliance, in action.

# Lead Practitioner & Trainer

**Amar Singh – Founder of Cyber** Management **Alliance Ltd, leading Global Cyber Security Executive and Lead Consultant**

Amar is a GCHQ-Certified trainer, industry influencer and is recognised globally as a leading risk management and data privacy professional. Organisations worldwide seek his input and thought leadership on matters related to cybersecurity and data privacy. Amar is regularly invited to speak internationally and deliver bespoke cyber resiliency workshops, executive and board briefings.

- Trusted advisor to police forces, financial institutions, hedge funds, banks, publishing houses, insurance companies, the NHS, housing associations and telecoms.
- Held Chief Information Security Officer positions at numerous organisations including Elsevier, News International, SABMiller, Gala Coral, Euromoney Institutional Investor and the BMJ Publishing Group.
- UK Government's GCHQ-Certified trainer and creator of IISP Accredited & GCHQ-Certified Cyber Incident Planning & Response Course (CIPR).
- Mentor to CISOs. Author, writer, industry speaker and presenter, guest lecturer at multiple universities and Chair of ISACA UK Security Advisory Group.
- Author and creator of UK Government-approved training course (CSPE).
- Author and creator of the Cyber Incident Planning & Response Workshop (CIPR).
- Author and creator of the Anatomy of Cyber Threats & Attacks Workshop for Security Analysts.
- (Former) judge for SC Magazine Awards & former Chair of ISACA's Security Advisory Group.