2016 CYBER SECURITY DEMYSTIFIED FOR THE BOARD AND COMPLIANCE

A programme of four workshops:

- WORKSHOP 1 → PROVIDE AWARENESS - 13TH SEPTEMBER
- WORKSHOP 2 → DEAL WITH SPECIFICS - 10TH OCTOBER
- WORKSHOP 3 → HIGHLIGHT THE ISSUES - 15TH NOVEMBER
- WORKSHOP 4 → SUGGEST SOLUTIONS - 13TH DECEMBER

REGISTRATION: 12:15PM (BUFFET LUNCH AVAILABLE)
STARTS: 12:30 - 2:00PM
VENUE: POMME D'OR HOTEL (PLEASE NOTE THIS IS A JERSEY ONLY EVENT)
COSTS: £50 PER PERSON PER WORKSHOP
CPD: 1.5HRS
REG ONLINE: TRAINING.COMSUREGROUP.COM/EVENTS

TARGET AUDIENCE

Directors, NEDs, Compliance Officers, Risk Officers, Regulators & anyone else who is responsible for protecting their (and their clients) data.

INTRODUCTION THE REGULATORY DRIVER

On the 22 February 2016 the Jersey Financial Services Commission (JFSC) issued a Dear CEO letter on cyber security and stated:

- The Board of Directors (or equivalent) of registered persons will take overall responsibility for ensuring that their firm adequately addresses cyber-security risks.

They further stated that as a minimum a registered person (the board) should:

1. Understand (and document) the risk of a cyber-attack on their business and take appropriate documented measures to mitigate this risk; the level and type of risk mitigation should be appropriate and proportionate to the type, potential impact and likelihood of the risks identified;
2. Have in place appropriate contingency arrangements that they can deploy in the event of a cyber-attack, for example maintaining service levels for clients or informing relevant parties about the attack and its impact;
3. Keep these matters under review and test their effectiveness at appropriate intervals.

BACKGROUND THE BUSINESS DRIVER

- Outside of the JFSC regulatory driver the purpose of these workshops is to get away from the perception that cyber is just a technology problem that can be solved entirely through engineering solutions. There is a tendency for boards to look at it, fear that it's too technical to understand, and then delegate the whole issue to technologists – who duly deliver some technological fixes.
- The trouble with that is that most cyber-attacks are not exclusively – or even mainly – technical in nature. People and processes are every bit as important. This is because attackers tend to exploit the credulity or laxity of their targets to achieve their ends. And while some can and do develop highly technical attacks, for the most part these are facilitated in some way by people or process weaknesses in their victims' defences.
- Most cyber-attacks start with social engineering: sending emails with tempting but malicious links or attachments, compromise of websites that targets might visit, and so on. In doing so, they exploit people: the culture, training, and integrity of your staff.

WORKSHOPS THE SOLUTION

In consideration of the regulatory and business drivers for protecting data, Ricky Magalhaes, Information Security Officer (bio below) will lead ***x4 Thought Leadership events*** on the approach and steps financial institutions and the boards of directors should take when managing cyber-risk. In doing so Ricky will show:

1. That cyber-risk can be managed by understanding it and balancing investment in mitigation against similar investments needed in the business.
2. This risk is a leadership and a management issue, rather than an issue simply for the IT department.
3. How to use the same governance approaches as they use in other parts of their business, which will require clear policies and standards, good management information and a sensible approach to compliance.

Comsure™

Comsure Compliance Limited 1 Bond Street, St Helier, Jersey JE2 3NP
Call. +44 (0)1534 626841 ***Email.*** info@comsuregroup.com www.comsuregroup.com

THOUGHT LEADERSHIP 1.5HR WORKSHOPS

Comsure

1 AWARENESS 13TH SEPTEMBER

- Big Picture
- Speed Networking
- Introduction to Cybercrime as it impacts the commercial world
- The three ages of computing and their impact on business today
- Review of global trends in cybercrime
- Social engineering vs. technical attack
- Case Study: Lessons from some well-known cybercrime prosecutions
- Jurisdictional and legal issues for law enforcement against cybercrime
- Future trends: Cloud, mobile, BYOD, cyber currencies and "Big Data"
- Enduring "best practices" that can still offer protection
- How businesses respond to Cybercrime incidents
- Outsourcing vs. insourcing of skills / infrastructure
- Discussion: What is "normal practice" in business now?

2 SPECIFICS 10TH OCTOBER

- Data vs. Information vs. knowledge vs. business value
- Review of common ICT operations and typical management practices
- How best to defend intangible assets
- Computer Forensics and penetration testing
- Case Study: Issues inherited with legacy IT systems
- Adoption of proven industry standards
- Examples of mandated controls
- Directors exposure to accusations of "gross negligence"
- Compliance issues related to Cybercrime
- Insurance for Cybercrime
- Prosecuting cybercrime incidents
- Discussion: Business culture vs. Cybercrime exposure

3 ISSUES 15TH NOVEMBER

- Cybercrime control options and costs
- Classifying data and controlling data distribution
- Matching internal controls to own operations
- Monitoring and modifying internal controls
- How to: Map your infrastructure and ICT supply chains
- Case Study: Risks inherent in new or upgraded IT systems

4 SOLUTIONS 13TH DECEMBER

- ***How to*** Develop a high level risk map for your business
- ***How to*** Identify key business dependencies and potential weakness
- ***How to*** Set your own cybercrime and business continuity strategy
- ***How to*** Review your ICT budget in view of risks and future plans
- ***How to*** Involve specialists and exploit freely available support

In each of these sessions Ricky will show how firms can balance cyber-risk against other risks through quantifying it, by breaking the risk down into:

- ***Threats*** - Ricky will outline the types of people that might want to launch a cyber-attack on a financial institution and their likely motives.
- ***Vulnerabilities*** - These are the weaknesses that can be exploited by attackers, including outdated operating systems, poor patching, untrained staff, unsegregated networks and weak security monitoring. A firm should treat any failings in its ability to respond to a critical incident as a vulnerability.
- ***Assets*** - These are the systems or information that underpin firms' critical business processes. Firms must identify these assets and have a clear view on the impact of their business if they are compromised. Ricky emphasises that the owners of the business processes that these assets support must be accountable for the cyber-risk relating to these assets.

RICKY MAGALHAES SPEAKER BIO

Ricky Magalhaes is a cyber-security expert and strategist for the past 17+ years working with the world's leading brands. Ricky sold his company to Evolve Networks in 2005 and joined the leadership of a large SI in the UK which was sold to the Datatec group (Logicalis) in 2012. Ricky leads the security division at Logicalis and is responsible for building together with the leadership the strategy for the European security operations.

Ricky is on multiple advisory boards for vendors, customers and cyber security industry bodies and periodically works with leading analyst firms to help device strategy and advice on cyber security. Full bio can be found on Comsure website: ***www.comsuregroup.com***