INTERNATIONAL SAIL TRAINING AND TALL SHIPS CONFERENCE 2018

SESSION 5E

CYBER SECURITY AWARENESS ONBOARD AND IN DAILY LIFE

Cyber Security Awareness onboard and in daily life

Stephan Kramer
Master Mariner, Compliance Consultant, DPA, STCW Trainer,

ROOD BOVEN GROEN | FOR ALL MARITIME AFFAIRS

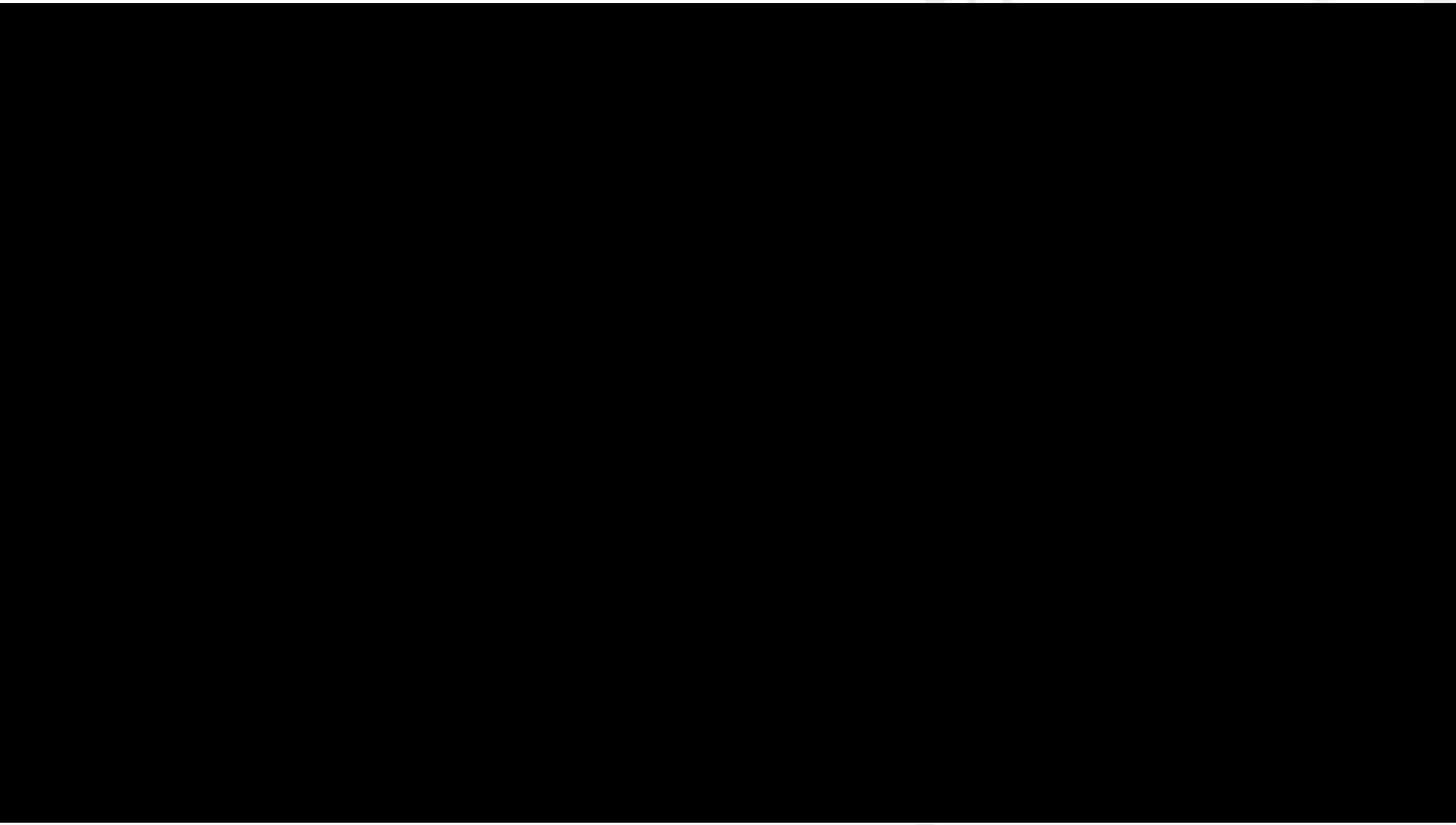
Sail Training International

Cyber Security Awareness onboard and in daily life

- History, Presence and Future
- Paradigma
- Human Factor

History, Presence and Future

- 1969 Neil Armstrong
- Computers and software in transport industry
- Autonomous Techniques
  - having the freedom to govern itself or control its own affairs



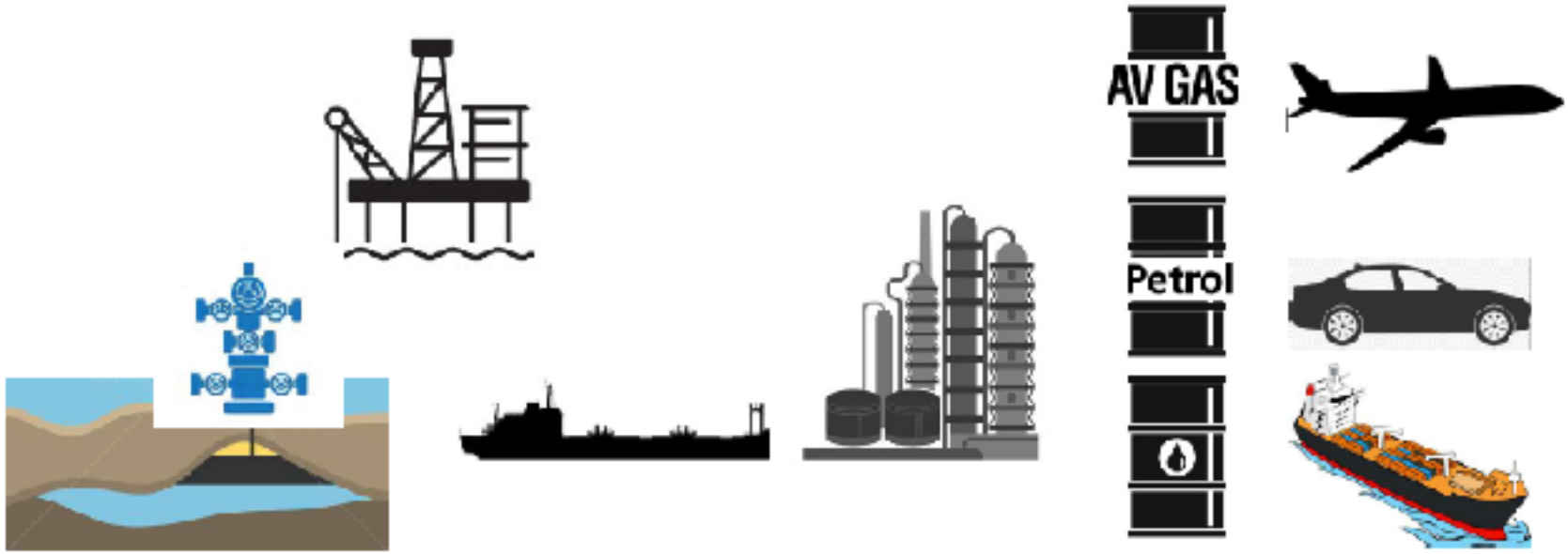
History, Presence and Future

History, Presence and Future

- If the service is for free, you are the product!

History, Presence and Future

Steps toward revealing data value



Paradigma

- www.kahoot.it

Paradigma

- Management of change

Paradigma

- Did you implement any kind of Cyber Security management to your company?

Paradigma

- Did you implement any kind of Cyber Security management to your fleet?

Paradigma

- Do you have an overview of your digital equipment onboard prone to Cyber Crime?

Paradigma

- How does Fleet broadband and/or VSAT broadband affect your communication?

Paradigma

- Do you have policies and procedures to address cyber crime inb your ISM, ISO and/or ISPS?

Paradigma

- What is your Cyber Security prevention and defense?

Paradigma

- If a ship Cyber Security event occurs, who is in charge? Whom to call?

Paradigma

- What are you actively doing to keep antivirus software, computer patches and systems updated onboard?

Paradigma

- Who is responsible for updating and who is monitoring log files?

Paradigma

- Are you using third party services and how do you know their capabilities/credits?

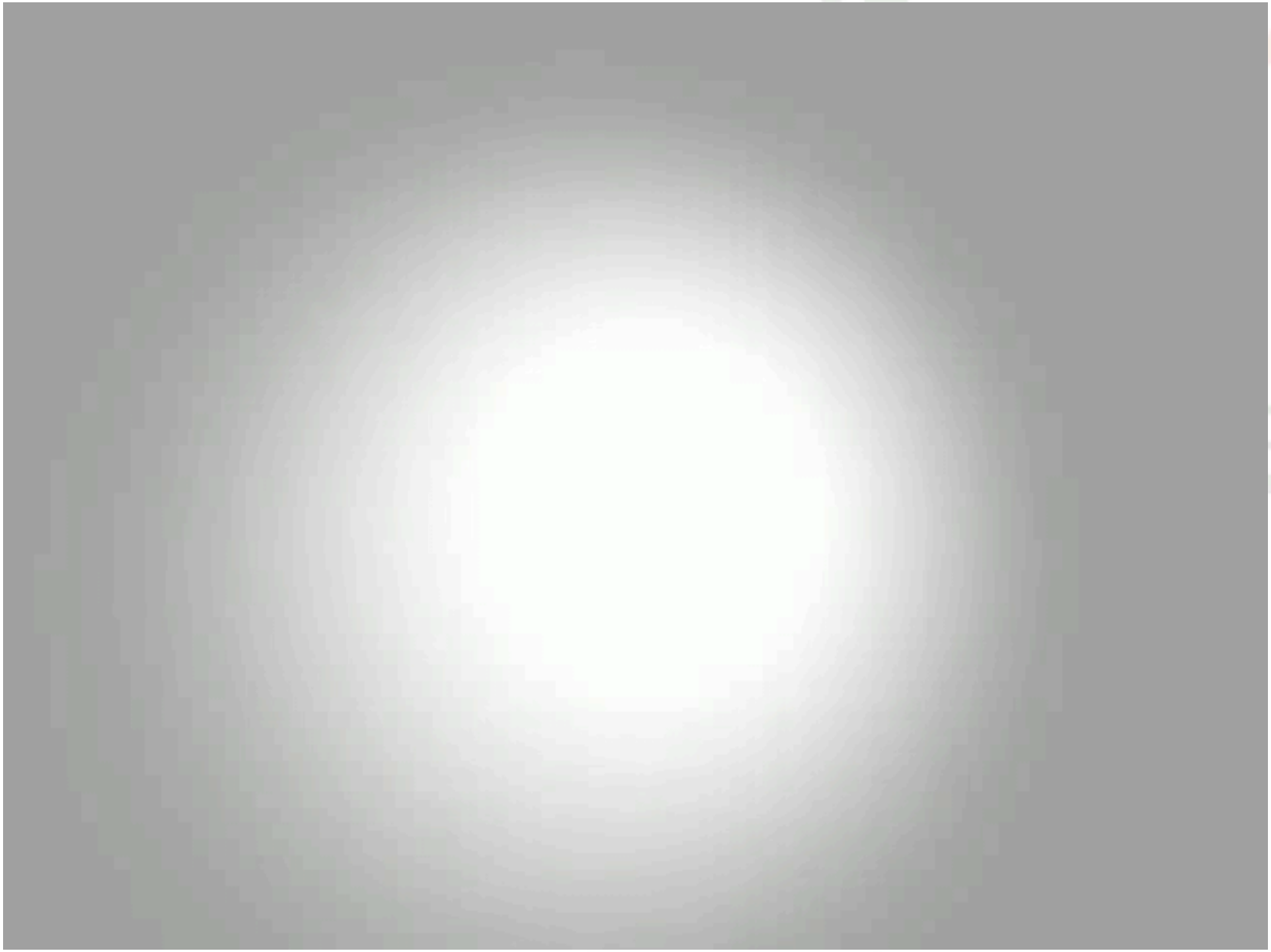
Paradigma

- Have you thought about what hardware to use and how to use? Think of external back-up devices, data blockers, usb ports blocked?

Paradigma

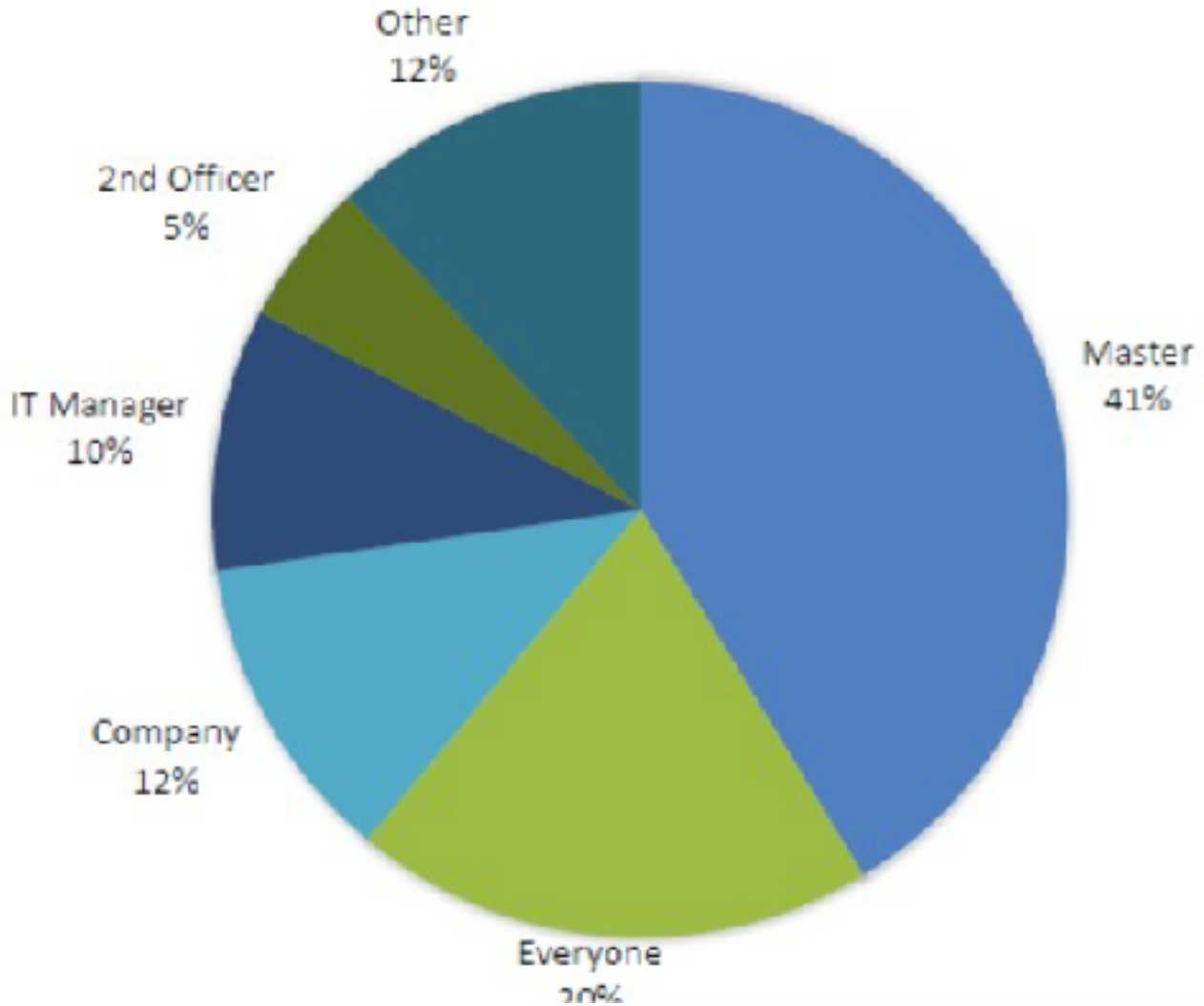
- How does your company address controlling and monitoring of save crew internet use?

HumanFactor



Human Factor

Human Factor



Human Factor

- *80 per cent of the cybersecurity incidents could have been prevented if single users were able to recognize the threat.*
- *It is vitally important to educate the crew on board in order to raise awareness about the vulnerabilities arising from human error.*

Human Factor

- People that can cause a cyber-breach are usually the ones that interact with the Information or Operational Technology such as:

- Shareholders/Owners • Management
- Employees
- Business Partners
- Service Providers • Contractors
- Customers/Clients

Human Factor

- Despite the arising danger, crew communications services are one of the most desired provisions for the onboard personnel.
- 75% of seafarers said the level of connectivity provided on board did influence which ship operator they worked for

- BYOD Bring your own device

Human Factor

- **E-mail** - Risks regarding e-mails and phishing scams should be de- clared, and examples of users clicking on malicious links should be simulated.
- **Web browsing** - having in an unwilling and unsafe manner during web browsing clicking on suspicious links should be avoided by the crew.
- **Removable media** - Infected USBs can be proven extremely danger- ous regarding cyber incidents. Today USB sticks are not only used to transfer data on board but also for updating critical systems such as the ECDIS system.

Human Factor

International initiatives and legislation

International initiatives

- Industry Round Table (BIMCO, ICS, Intertanko, Intercargo and CLIA) Guidelines on Cyber Security on board Ships
- IMO Interim Guidelines on Maritime Cyber Risk Management adopted by MSC 96 in May 2016 and are largely based on Industry Round Table Guidelines
- Be Cyber Aware At Sea campaign (www.becyberawareatsea.com)
- Cybersail (https://cybersail.org)
- CSO Alliance (www.csoalliance.com)
- IACS Classification Societies providing assistance to protect security of shipboard cyber-enabled systems
- P&I clubs loss prevention
- OCIMF vetting inspections

Human Factor

INTERNATIONAL MARITIME ORGANIZATION

E

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210

MSC.1/Circ.1526
1 June 2016

INTERIM GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

1 The Maritime Safety Committee, at its ninety-sixth session (11 to 20 May 2016), having considered the urgent need to raise awareness on cyber risk threats and vulnerabilities, approved the *Interim guidelines on maritime cyber risk management*, as set out in the annex.

2 The Guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

3 Member Governments are invited to bring the contents of this circular to the attention of all stakeholders concerned.

Human Factor

"'Be careful'! All you can tell me is 'be careful'?"

Human Factor

Thank you