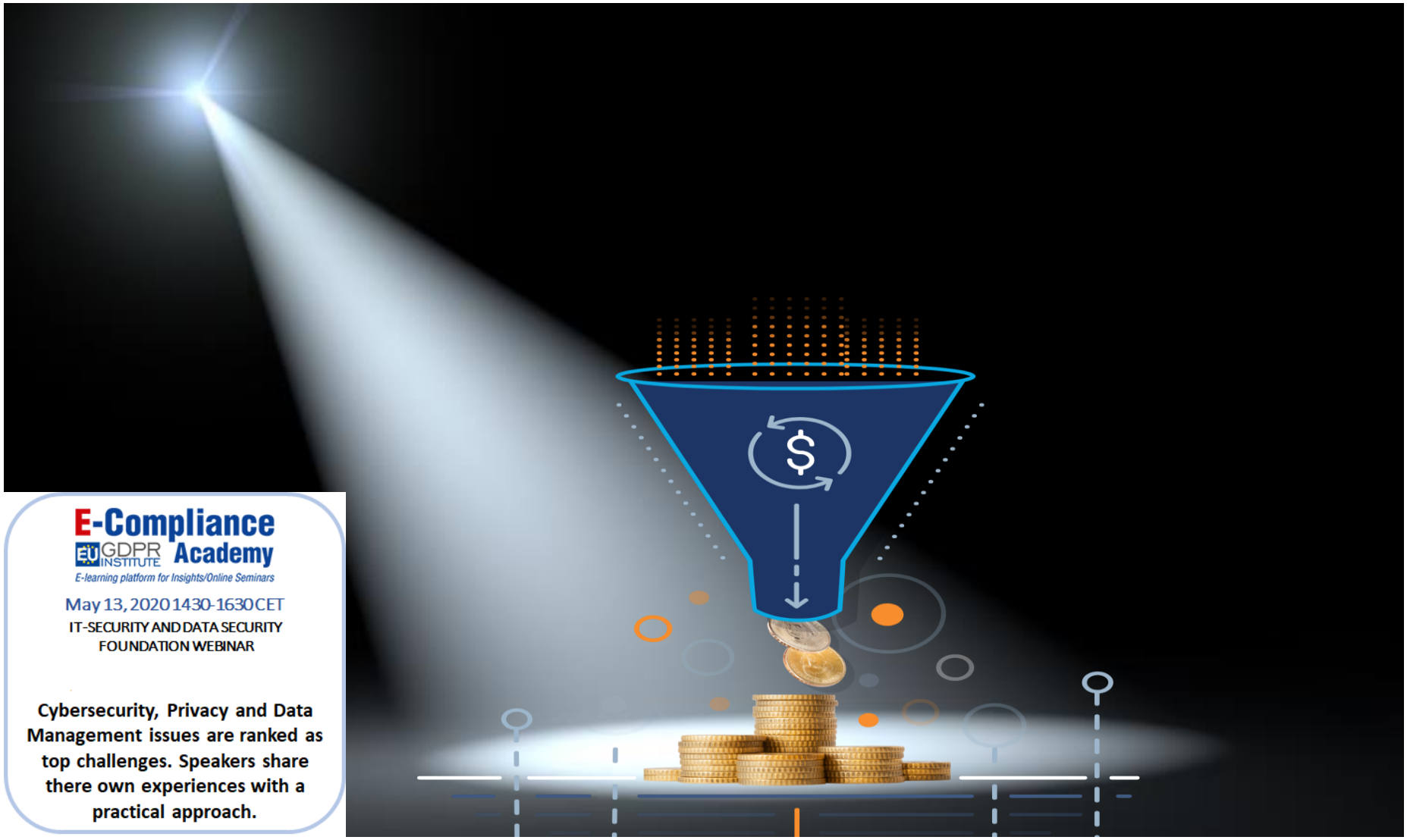
Welcome and Introduction

COPENHAGEN COMPLIANCE



E-Compliance
EU GDPR INSTITUTE Academy
E-learning platform for Insights/Online Seminars

May 13, 2020 1430-1630 CET
IT-SECURITY AND DATA SECURITY
FOUNDATION WEBINAR

Cybersecurity, Privacy and Data Management issues are ranked as top challenges. Speakers share there own experiences with a practical approach.

Online Webinar 13th May 2020

Kersi F. Porbunderwala, CEO, The EUGDPR Institute

E-Compliance Academy
E-learning platform for Insights/Online Seminars

COPENHAGEN COMPLIANCE

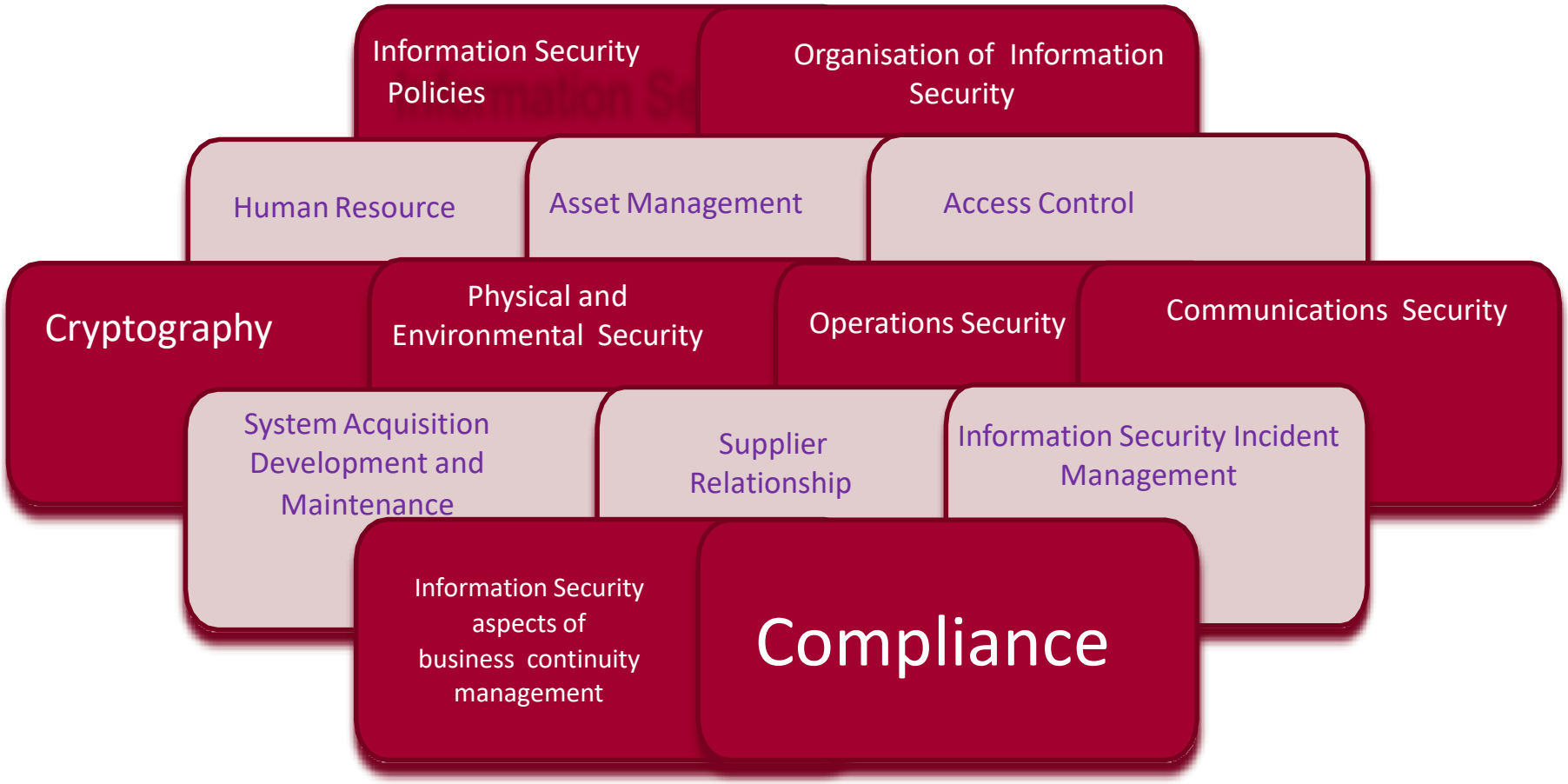
- **The Importance of Data Security, IT Security and Cybersecurity.**
- ***Review of best practices to secure the business against fraud, ransomware, phishing, data mining and other attacks on your systems and data.***

Agenda

- **What Is Cyber Security**
  - Information Technology Security (IT Security) Or Electronic Information Security (EIC)
- The Scale Of The Cyber Threats
- **Practical Steps And Checklist For Responding To The Coronavirus Crisis.**
  1. The Organisation
  2. The Employees
  3. The Senior Management
  4. The Board Of Directors
- **Security Awareness Training**
- **Disaster Recovery And Business Continuity**

IT Security Compliance Components

COPENHAGEN COMPLIANCE



Source: Domains of Information Security (114 Controls in ISO 27002)

IT-& Data Security and (EIC) Electronic Information Security

COPENHAGEN COMPLIANCE

1

Data security

- Encryption
- Access control
- Tokenization

2

IT security

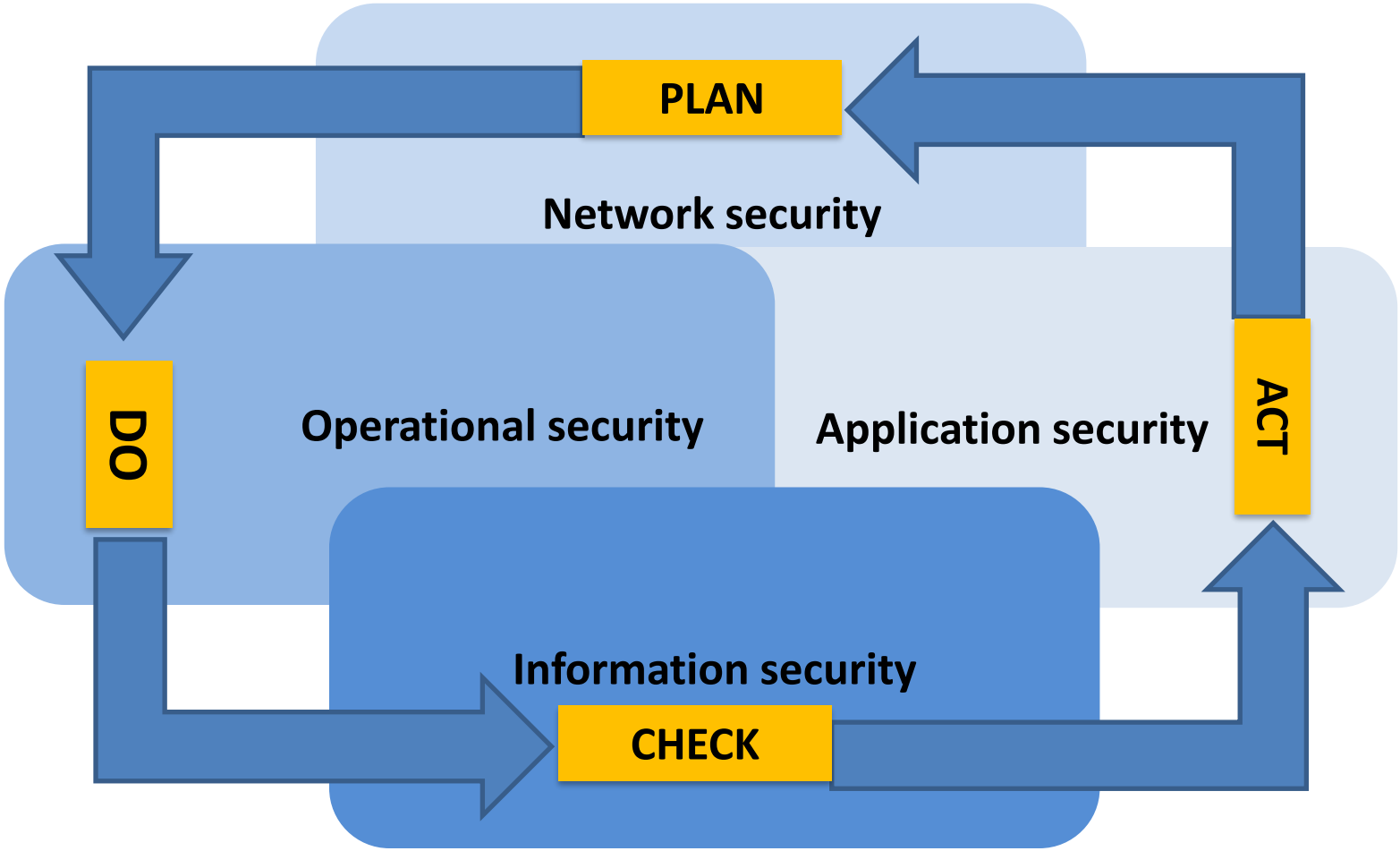
- Backups
- Patches
- Antivirus

3

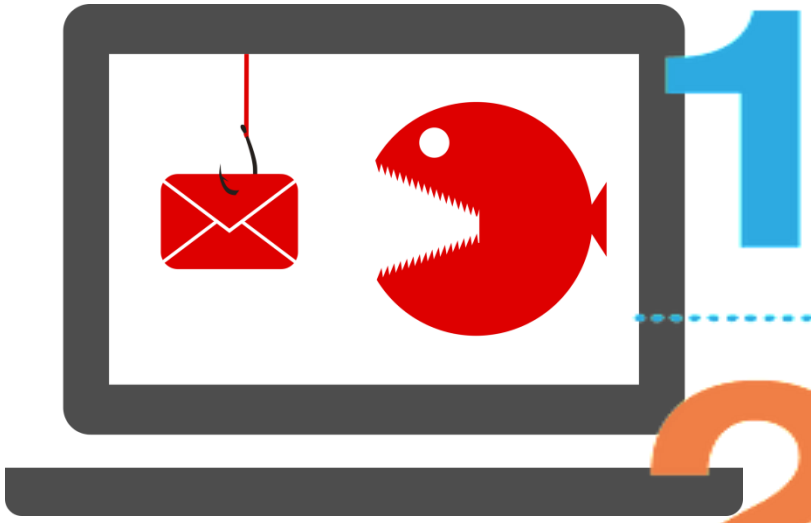
Cyber security

- Response plans
- Awareness
- Defense

Cyber Security Context



Three threats of cyber-security



1

Cybercrime
includes single actors or groups targeting systems for financial gain or to cause disruption.

2

Cyber-attacks
Are often involves politically motivated information gathering

3

Cyberterrorism
is intended to undermine electronic systems to cause panic or fear.

https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en

The global scale of the cyber threat

The Organisation

01 Assess Core IT Infrastructure For Remote Working

02 Secure Applications And Devices For The Remote Workforce

03 Embed Cybersecurity Into Business Continuity Plans

04 The *Newly* Remote Workforce Aware Of The All Security Risks

05 Establish Protocols And Behaviours For Secure Remote Working

06 Embed Cybersecurity In Corporate Crisis Management

07 Update Access And Security Measures

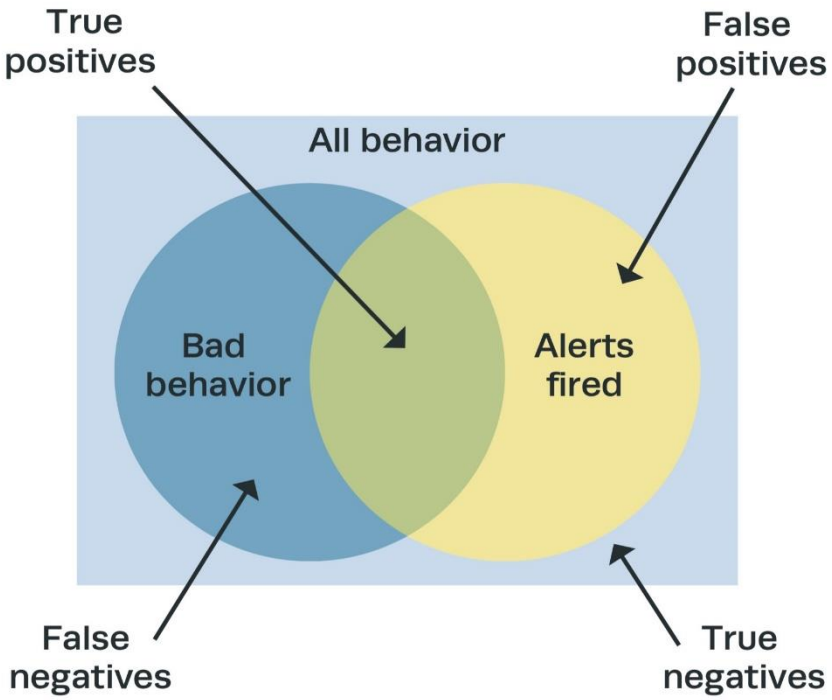
The Employees' Cyber safety tips

1. Update software and operating system for benefit from the security patches
2. Use anti-virus software, multiple security solutions to detect and removes threats.
3. Use strong uncommon passwords
4. Do not open email attachments from unknown senders
5. Do not click on any links from unknown senders or unfamiliar websites
6. Avoid using unsecure Wi-Fi networks in public places

The Employees' Cyber safety tips

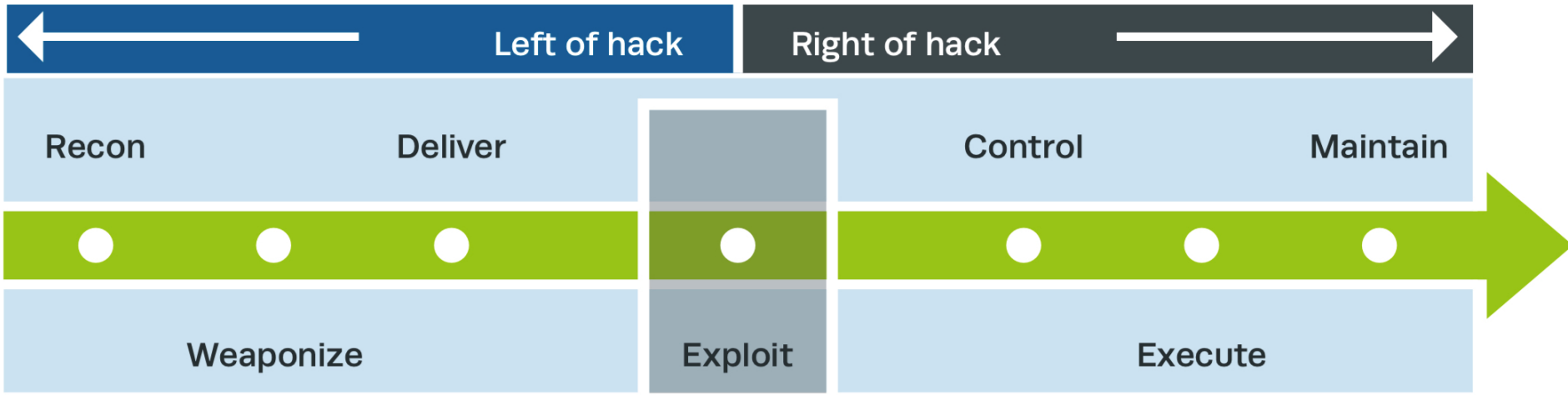
- Emails masquerading as government announcements
- Operational and industry disruption
- Hidden malware
- False advice and cures
- False charity
- Fraud that go beyond business email compromise

The SHARP Problems for Executive Management



1. Consolidate the SHARP; (Security, Human, Application, Risk) Processes
   Addresses the functions of incident, monitoring, detection, and response
2. Achieve balance between size and visibility/agility, so that the SHARP can execute its mission effectively
3. SHARP has the authority to ensure effective organisational placement & appropriate policies/ procedures
4. Focus on a few activities that the SHARP practices well and avoid the ones it cannot or should not be done
5. Support staff quality over quantity.
   passionate professionals with a balance of soft and hard skills, will pursue growth opportunities

The *SHARP* Problems for Executive Management



Cyber Attack Life Cycle

6. Realise full potential of technology from investment in system/tool's & limitations.
7. Exercise care in the assignment of devices, collection of data, and maximising non compliance indicators
8. Protect SHARP systems, infrastructure, and data with transparent and effective communication
9. Ensure cyber threat intelligence, reporting, incident management
10. Respond to cyber incidents in a calm, calculated, and professional manner

The *SHARP* Problems For Board Of Directors

COPENHAGEN COMPLIANCE

01 Does the board understand the company's total risk exposure of a cyber attack, including financial, legal and reputational impacts?

02 Has the board practiced a cyber breach simulation with management in the last year? If not, why?

03 Evaluate the corporate culture to cybersecurity? Employee training, security awareness, performance bonuses…

04 Leverage and meet the objectives of third-party expertise, Cyber-Risk Oversight, validate the risk management program

05 Information to assess which critical business assets and critical partners, including third parties and suppliers, most vulnerable to cyber attacks?

06 Is an appropriate and meaningful cyber metrics been identified and provided to the board on a regular basis on a given dollar value?

The *SHARP* Problems For Board Of Directors

COPENHAGEN COMPLIANCE

07 Evaluate the process used to assess a comprehensive view of cyber risk management program by a third party

08 Is management's supervision of critical vulnerabilities adequate and how often are they performed

09 Has management indicated where the next cybersecurity dollars should be invested and why?

10 How is the company handling privileged access and how do they oversee employees with privileged access, including superusers?

11 Is the policy for publicly- disclosed breaches based on a scenario plan? What are the lessons learned from incidents and are they incorporated in a response plan?

12 How does management evaluate and categorise identified incidents and benchmarked/thresholds which ones to escalate to the board?

Awareness Training, Disaster Recovery & Business Continuity

Security awareness training

- The end-user is not the most unpredictable cyber-security factor
- Educate on good security practices with important lessons and examples
- Data breaches are directly or indirectly caused by user awareness issues
- Promote security awareness training initiatives, encouragement, duty and accountability to make the organisation safe or less vulnerable.

Disaster recovery and business continuity

- Define the response to a any incident or event that causes the loss of operations or data.
- Disaster recovery policies dictate on restoring operations and information
- Business continuity plan to operate without certain resources.

Thank you. See you on the 25th May

COPENHAGEN COMPLIANCE

E-Compliance Academy

E-learning platform for Insights/Online Seminars

E-seminars, webinars, Training and Awareness

https://www.copenhagencompliance.com/2020/annual/register.htm

EU GDPR INSTITUTE

Data Privacy, Data Protection, Training and Certification

COPENHAGEN COMPLIANCE Global GRC Solutions

Conference, Consultancy, Communications

information security institute

IT-Governance, Information-Security, Cyber Security

COPENHAGEN, DENMARK
DTU Science Park
Technical University of Denmark, Diplomvej 381,
DK-2800 Lyngby, Denmark

LONDON, UK
Copenhagen Compliance UK Ltd.
21 Cloudesley Street London N1 0HX
United Kingdom

MUMBAI, INDIA
DadySheth House 2nd floor, Plot 44,
Cawasji Patel Road, Horniman Circle,
Fort, Mumbai -400001

PORTLAND, USA
13330 NW Old Germantown Road.
Portland, Oregon 97231.
USA

E-Mail:info@eugdpr.institute or info@information-security.institute.Tel: Europe: +45 21210616/ Asia: +91 9920801838