COPENHAGEN COMPLIANCE
Global GRC Solutions

GDPR's operation has revealed progress in how personal data is protected across the digital domain

Emmanuel Fragnière

University of Applied Sciences Western Switzerland

EDPS
European Data Protection Supervisor

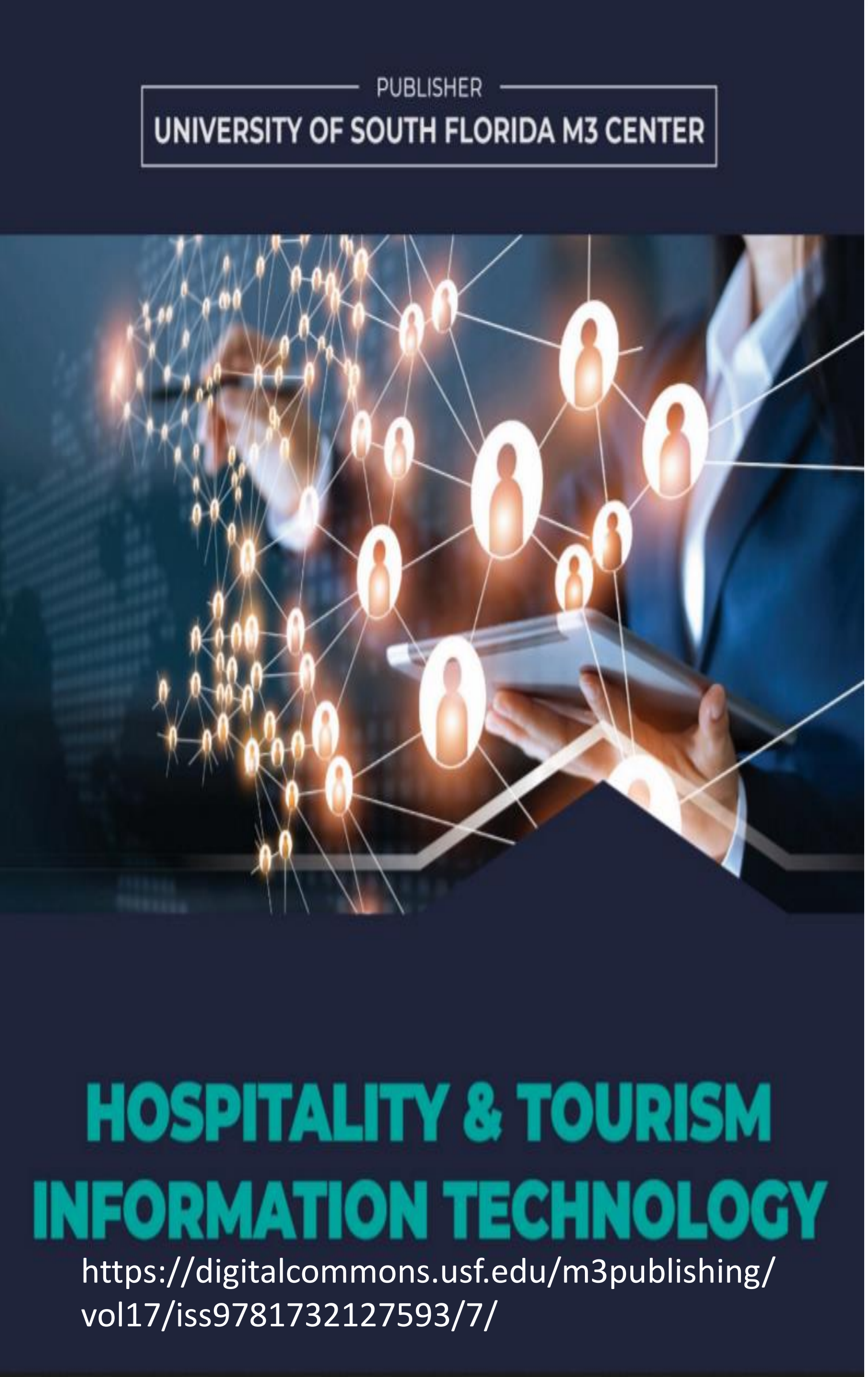
"THE FUTURE OF DATA PROTECTION: EFFECTIVE ENFORCEMENT IN THE DIGITAL WORLD"

EDPS 2022 CONFERENCE
16-17 JUNE 2022

edps.europa.eu

Global
Data Protection
Day
by Copenhagen Compliance

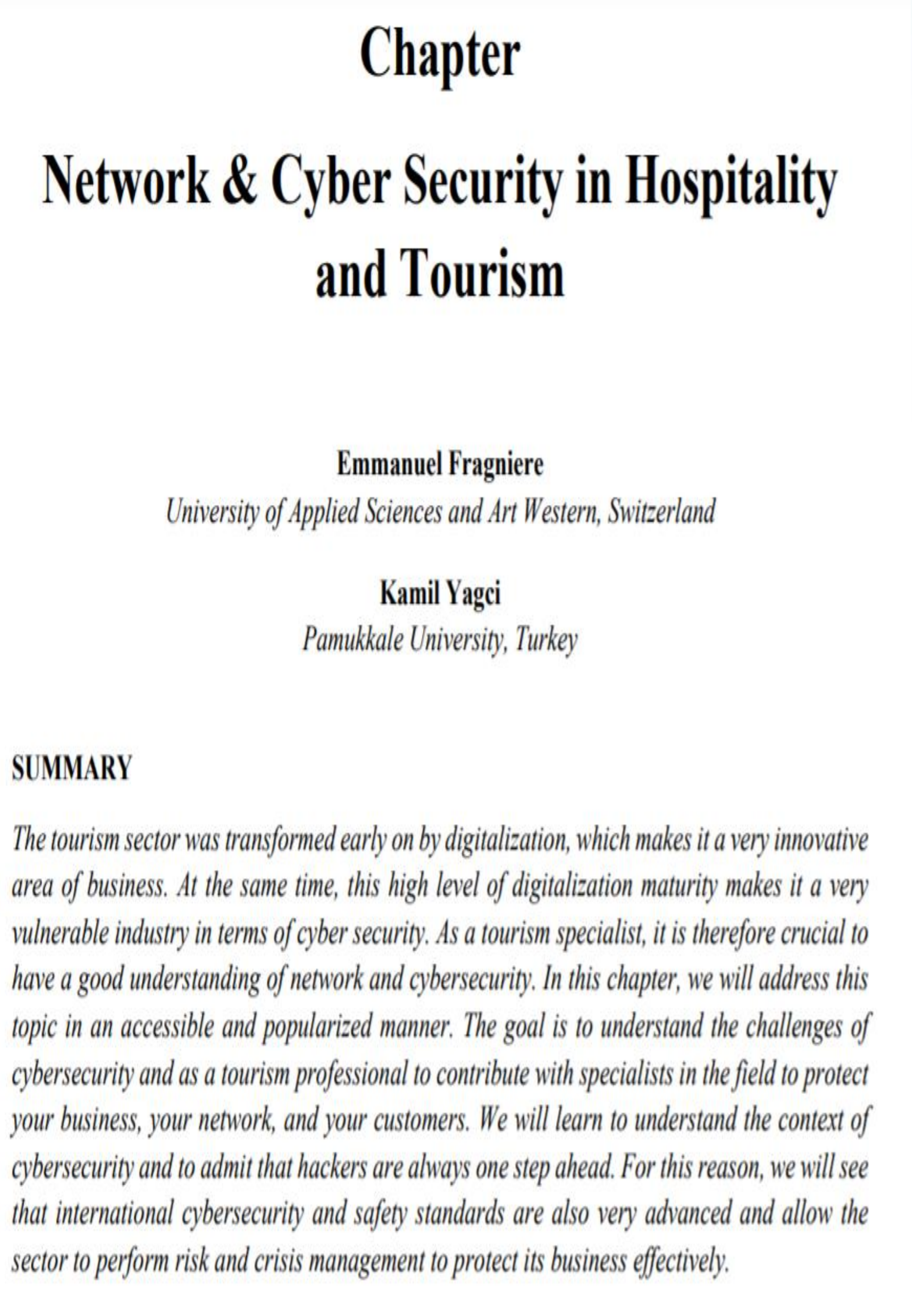
JANUARY 28, 2022
ONLINE CONFERENCE



PUBLISHER
UNIVERSITY OF SOUTH FLORIDA M3 CENTER

HOSPITALITY & TOURISM INFORMATION TECHNOLOGY

https://digitalcommons.usf.edu/m3publishing/vol17/iss9781732127593/7/



Chapter

Network & Cyber Security in Hospitality and Tourism

Emmanuel Fragniere
University of Applied Sciences and Art Western, Switzerland

Kamil Yagci
Pamukkale University, Turkey

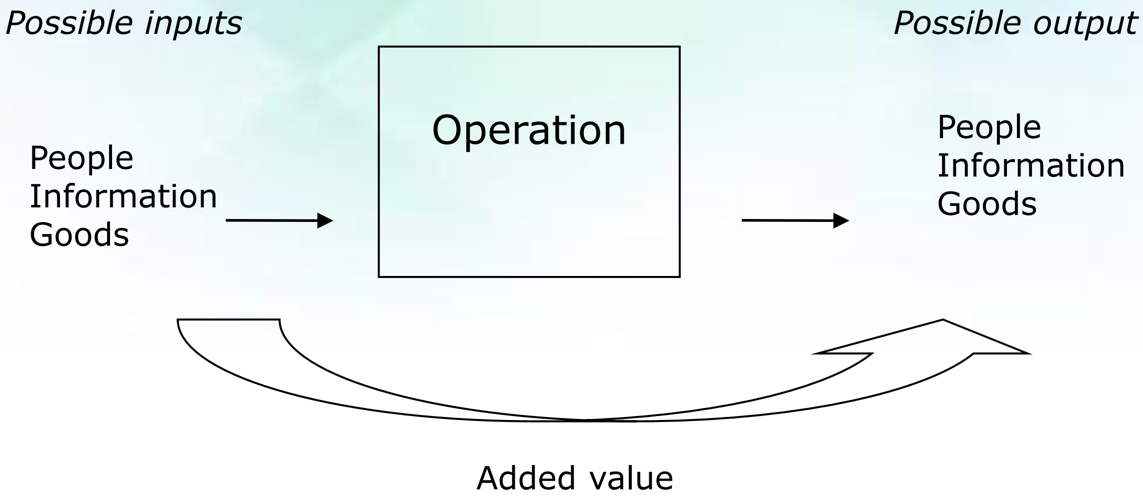
SUMMARY

The tourism sector was transformed early on by digitalization, which makes it a very innovative area of business. At the same time, this high level of digitalization maturity makes it a very vulnerable industry in terms of cyber security. As a tourism specialist, it is therefore crucial to have a good understanding of network and cybersecurity. In this chapter, we will address this topic in an accessible and popularized manner. The goal is to understand the challenges of cybersecurity and as a tourism professional to contribute with specialists in the field to protect your business, your network, and your customers. We will learn to understand the context of cybersecurity and to admit that hackers are always one step ahead. For this reason, we will see that international cybersecurity and safety standards are also very advanced and allow the sector to perform risk and crisis management to protect its business effectively.

Art. 4 GDPR
Definitions

(2) ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

What is an operation?



Possible inputs

People
Information
Goods

Operation

Possible output

People
Information
Goods

Added value

A digitalized banking operation

Source : n26

COPENHAGEN COMPLIANCE
Global GRC Solutions

The online services evolution

- Customers are demanding new online services and innovative products, forcing the sector to review its product portfolio and innovate by implementing new technologies.
- This digital transformation increases the surface area of attacks and company networks more vulnerable to cyber-attacks.

GDPR’s operations within digital operations (examples)

- How do you protect stored data GDPR?
- Luckily there are a few basic principles you can follow.
- Physical security: locking doors, adding alarms.
- Digital security: passwords and encryption.
- Proper training: educate your employees.
- Restrict access: keep everything 'need to know'

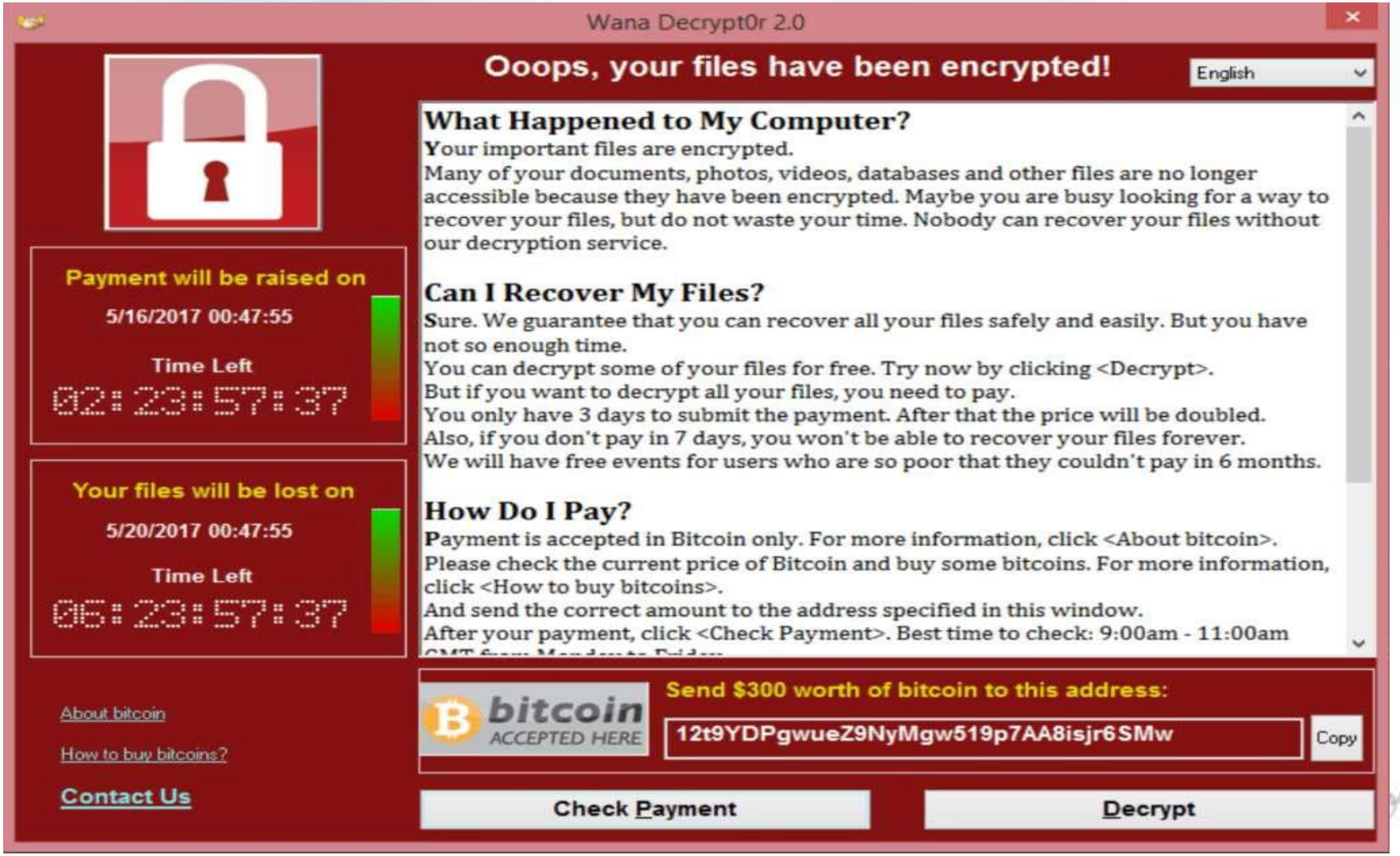
Source: https://www.iconography.co.uk/gdpr-guide-protecting-and-securing-data

COPENHAGEN
COMPLIANCE
Global GRC Solutions

Personal Data breach!

- “The **Marriot Hotel Group** has received a significant fine for failing to protect the personal data of its customers. Indeed nearly 340 million of customer account were concerned by this cyberattack. And even if the amount to be paid was finally lowered to about 20 million euros, let's not forget that the **image damage is huge**. “
- “**Bristish Airways** has also been fined (22 million euros) for leaving vulnerabilities in its customer database of over 400,000 accounts vulnerable to cyber-attacks. The worst thing is that this **BA network vulnerability remained "open" for almost 2 months** without the company being aware of it. The image risk is important. But let's not forget that cyber-attacks could also affect critical facilities such as power plants, hospitals, air traffic control centers.”

Infamous Image Seen when Hacked by the WannaCry Ransomware



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

The Geneva-based International Committee of the Red Cross (ICRC) has been the victim of a "sophisticated cyber-attack". Servers hosting the personal and confidential data of more than 515,000 extremely vulnerable people have been compromised.

January 20, 2022 - 09:23

ICRC/RTS/Reuters/sb

Other languages: 2 (EN original)

Share this story

The humanitarian organisation said on Wednesday that the breach by unknown intruders this week affected the data of hundreds of thousands of people "including those separated from their families due to conflict, migration and disaster, missing persons and their families, and people in detention".

Data protection 'shake-up' takes aim at cookie pop-ups

26 August 2021 BBC

- **The UK's new Information Commissioner will be charged with a post-Brexit "shake up" of data rules, including getting rid of cookie pop-ups.**
- John Edwards has been named the next head of data regulator the ICO.
- The government said Mr Edwards, currently the New Zealand Privacy Commissioner, would "go beyond the regulator's traditional role".
- **The job would now be "balanced" between *protecting rights* and promoting "*innovation and economic growth*".**
- Mr Edwards has been named as the government's preferred candidate, and said it is a "great honour".
- "I look forward to the challenge of steering the organisation and the British economy into a position of international leadership in the safe and trusted use of data for the benefit of all," he said.

Data Protection officer (DPO)

According to the GDPR, **a business/organisation** is responsible for complying with all data protection principles and is also responsible for demonstrating compliance. The GDPR provides businesses/organisations with a set of tools to help demonstrate accountability, some of which have to be mandatorily put in place.

The principle of **accountability** is a cornerstone of the General Data Protection Regulation (GDPR). According to the GDPR, a business/organisation is responsible for complying with all data protection principles and is also responsible for demonstrating compliance. The GDPR provides businesses/organisations with a set of tools to help demonstrate accountability, some of which have to be mandatorily put in place.

For example, in specific cases the establishment of a DPO or conducting data protection impact assessments (DPIA) may be mandatory. Data controllers can choose to use other tools such as codes of conduct and certification mechanisms to demonstrate compliance with data protection principles.

Source: https://ec.europa.eu/

COPENHAGEN COMPLIANCE
Global GRC Solutions

«Logic of enforcement»

To comply with GDPR, companies must adhere to several rules, including robust consent requirements, **privacy by design, and mandatory breach notifications**. The law extends several rights to users to access and control their data, including data portability and the 'right to be forgotten.

Source: https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement , 13 sept. 2021

Art. 33 GDPR
Notification of a personal data breach to the supervisory authority

[1]In the case of a personal data breach, the controller shall without undue delay and, **where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55**, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. [2]Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

One-Stop-Shop (OSS) and Security Operation Center (SOC)

What is GDPR one-stop-shop? A 'one-stop-shop' is usually **a business offering multiple services all under one roof**. From the GDPR perspective, the 'one-stop shop' is **a single contac**t point mechanism whereby companies doing business in more than one EU member state will deal with a 'lead' Data Protection Authority (DPA). Source: https://www.cookielawinfo.com/

A Security Operation Center (SOC) is a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents. A SOC acts like the hub or central command post, taking in telemetry from across an organization's IT infrastructure, including its networks, devices, appliances, and information stores, wherever those assets reside. The proliferation of advanced threats places a premium on collecting context from diverse sources." Source: mcafee antivirus

COPENHAGEN COMPLIANCE
Global GRC Solutions

BCM International standards

ISO 31000, COSO 2013

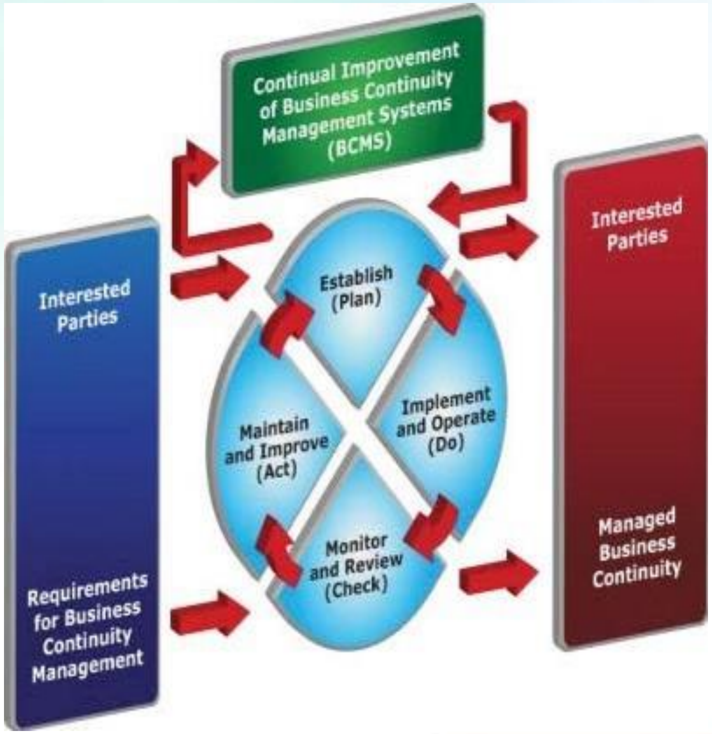
Risk management, internal control

ISO 22301 (superseding BS 25999)

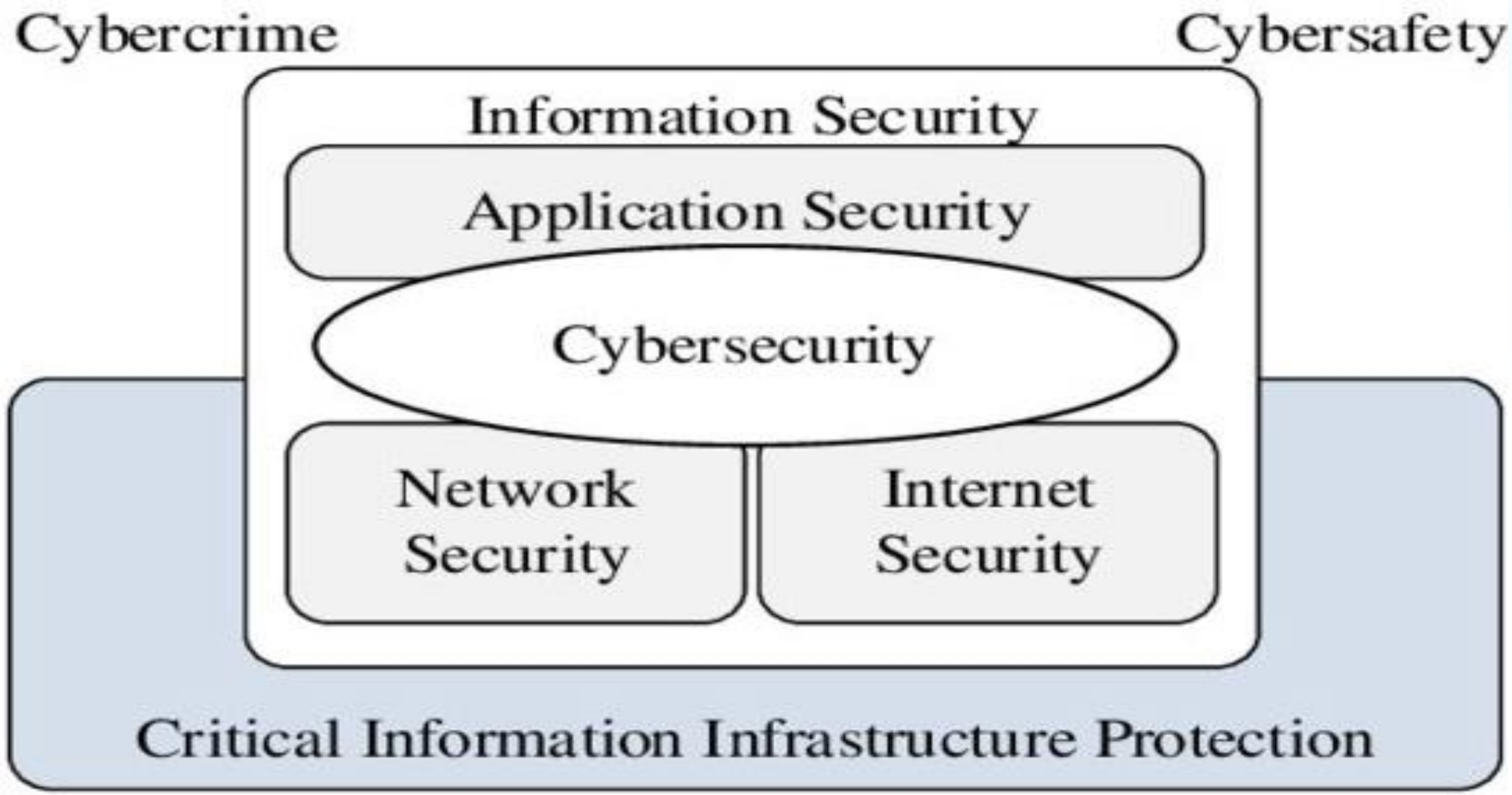
Business Continuity Management

ISO 27031

IT continuity, Disaster Recovery Planning


Continual Improvement of Business Continuity Management Systems (BCMS)
Interested Parties
Requirements for Business Continuity Management
Establish (Plan)
Implement and Operate (Do)
Monitor and Review (Check)
Maintain and Improve (Act)
Interested Parties
Managed Business Continuity

The Link Between Cybercrime and Cybersafety Through Cybersecurity as Defined by ISO/IEC 27032



COPENHAGEN COMPLIANCE
Global GRC Solutions

Algorithms vs human factor!

This brings us to the notion of **social engineering**. Any cybersecurity specialist will tell you that the weakest link is always human. So, a cybersecurity specialist will of course have to know how to program in **python**, **Java** or **C/C++** to perform an **intrusion test**.

But this technical skill is a necessary but not sufficient skill. In order to make the difference, the cyber security specialist must have competence in psychology and sociology. Indeed, social engineering is also called **psychological fraud**.

Conclusions

“COVID has forced millions of people to work at home and in a totally improvised way. At the same time, the number of computer breaches has never been so high. Here we see that while serious companies are doing quality cyber resilience work, suddenly it's as **if everyone working at home has let their guard down**.”

“Also, think about regularly updating these antiviruses and follow the instructions provided by your company. In the end, a good **cyber hygiene** as we all have a good health hygiene must nowadays be part of our daily life.”

https://www.cisa.gov/cyber-resource-hub

COPENHAGEN
COMPLIANCE
Global GRC Solutions

?