Dall'Information Security alla Cyber Security, e ritorno

(Come migliorare la sicurezza dell'azienda attraverso un efficace governo degli incidenti)

Luca Bechelli (CLUSIT)
Marco Di Leo (HP)
Fabio Vernacotola (HP)

Dall'Information Security alla Cyber Security

Luca Bechelli
Direttivo CLUSIT
luca@bechelli.net
www.bechelli.net

Cosa si intende per Cyber**Security**

Cobit: Transforming Cybersecurity: Using COBIT® 5

cybersecurity |ˌsībərsiˈkyo͝oritē| :

"…cybersecurity encompasses **all that protects enterprises and individuals from intentional attacks, breaches and incidents as well as the consequences**.
In practice, cybersecurity addresses primarily those types of attack, breach or incident that are targeted, **sophisticated and difficult to detect or manage**.
The much larger field of opportunistic attacks and crime usually can be dealt with using simple but effective strategies and tools. As a result, **the focus of cybersecurity is on what has become known as advanced persistent threats** (APTs), **cyberwarfare** and their impact on enterprises and individuals…"

Cosa si intende per Cyber**Security**

US National Initiative for Cybersecurity Careers and Studies (NICCS)

cybersecurity |ˌsībərsiˈkyo͝oritē| :

The activity or process, ability or capability, or state whereby information and communications **systems and the information** contained therein are protected from and/or defended against **damage**, **unauthorized** use or **modification**, or **exploitation**

Cosa si intende per Cyber**Security**

NIST IR 7298 Revision 2, *Glossary of Key Information Security Terms*

cybersecurity |ˌsībərsiˈkyo͝oritē| :

The ability to protect or defend the use of **cyberspace** from **cyber attacks**.

Or

The **process** of protecting information by **preventing**, **detecting**, and **responding** to **attacks**.

Cyberspace:
A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Cyber Attack:
An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/ infrastructure; or destroying the integrity of the data or stealing controlled information

Cosa si intende per Cyber**Security**

TechTarget "What is" section

cybersecurity |ˌsībərsiˈkyo͝oritē| :

"Cybersecurity is the body of technologies, processes and practices designed to **protect** networks, computers, programs and data from **attack, damage or unauthorized access**.

In a computing context, the term **security implies cybersecurity**"

CyberSecurity & **Information**Security

Information Security

Cyber Security

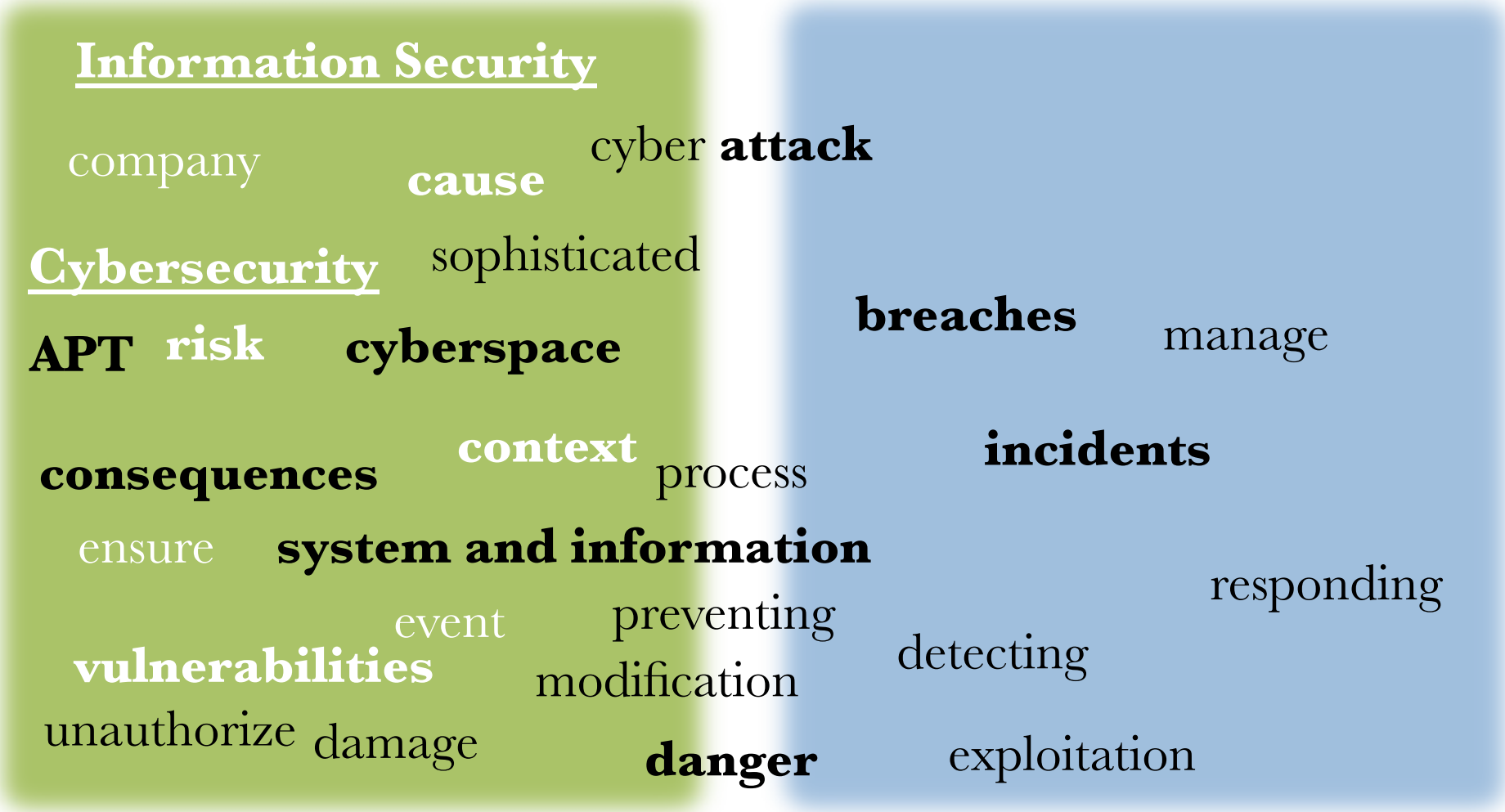
80114.

Trova l'intruso

cybersecurity
guarantee
cyber **attack**
identify
sophisticated
vulnerabilities
APT
cyberspace
breaches
manage
risk
consequences
process
incidents
company
event
system and information
context
responding
danger
preventing
unauthorize
detecting
modification
cause
damage
exploitation
ensure

ORIZZONTALI

CyberSecurity & **Information**Security



CyberSecurity & **Information**Security

The National Cyber Security Strategy 2011, Dutch Ministry of Security and Justice

cybersecurity |ˌsībərsiˈkyo͝oritē| :

"The definition of **Cybersecurity** is not far from information security:

> *Cybersecurity is to be **free from danger or damage** caused by **disruption** or fall-out of ICT or **abuse** of ICT.*
>
> *The danger or the damage due to abuse, disruption or fall-out can be comprised of a **limitation of** the availability and reliability of the ICT, **breach of** the confidentiality of information stored in ICT or **damage to** the integrity of that information."*

Il perimetro

Information Security

Proteggere

Riservatezza

Integrità

Disponibilità

Sistema Informativo

Cyber Security

Difendere da

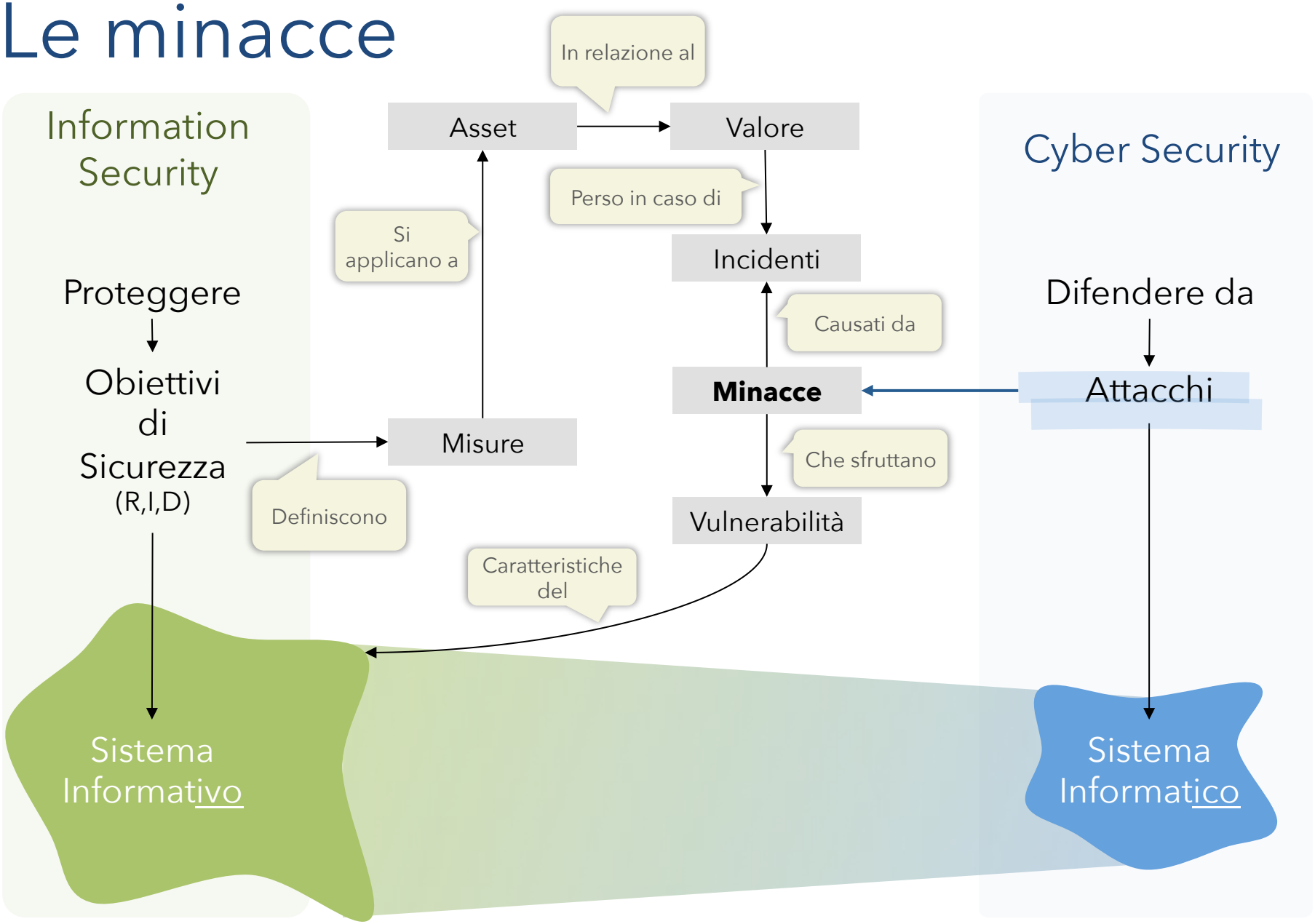
…breach of the **confidentiality** of information stored in ICT…

…damage to the **integrity** of that information…

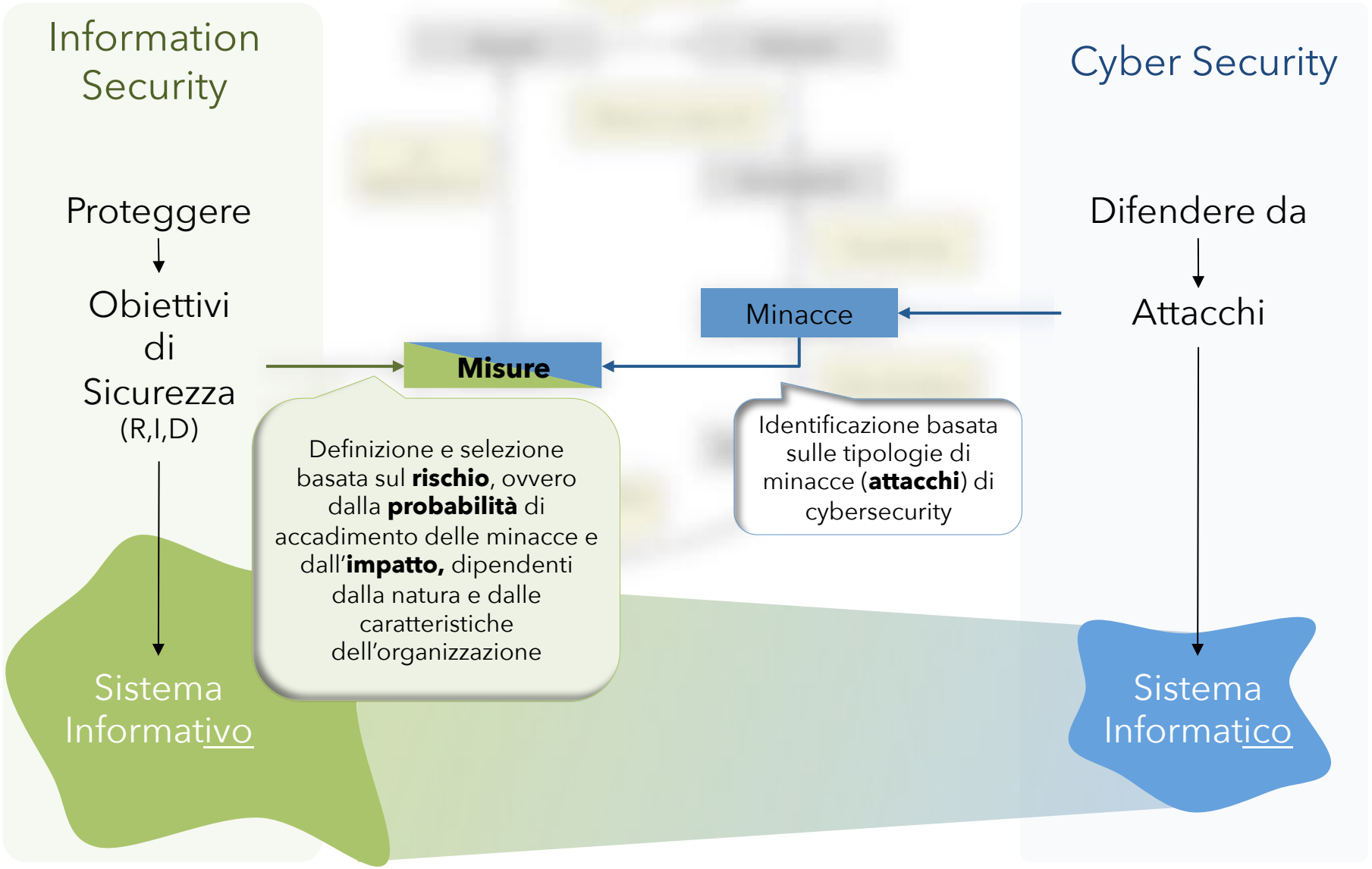
…limitation of the **availability** and reliability of the ICT…

Sistema Informatico

Le minacce


Information Security
Cyber Security
In relazione al
Asset
Valore
Perso in caso di
Si applicano a
Incidenti
Proteggere
Causati da
Difendere da
Obiettivi di Sicurezza (R,I,D)
Minacce
Attacchi
Misure
Che sfruttano
Definiscono
Vulnerabilità
Caratteristiche del
Sistema Informativo
Sistema Informatico

Contromisure



Abbiamo bisogno di CyberSecurity?

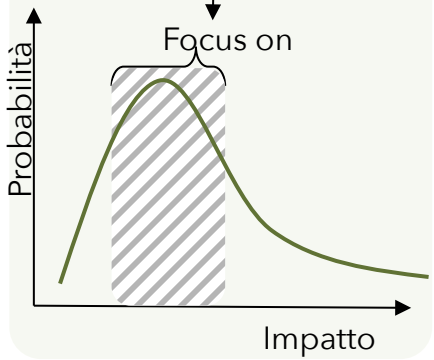
Information Security

Contesto

Rischio

"ieri"

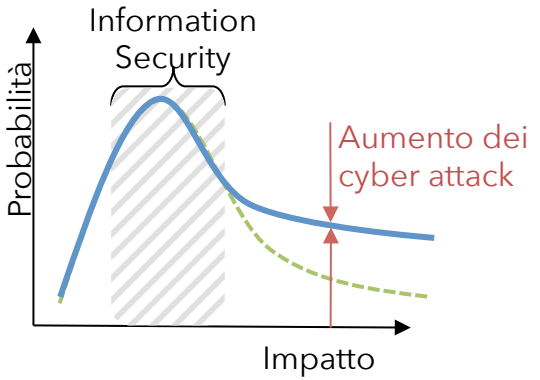
- Storico degli eventi
- Benchmark di settore
- Metriche Retrospettive
- "eventi immaginati"



…security attacks in the Cyberspace have evolved from hacking for personal fame to […] Cybercrime. A plethora of tools and processes previously observed in isolated Cybersecurity incidents are now being used together in multi-blended attacks, often with far reaching malicious objectives

ISO 27032:2012

"oggi"



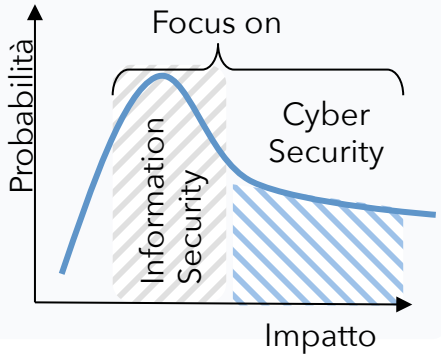
Cyber Security

CyberSpace

Attacchi

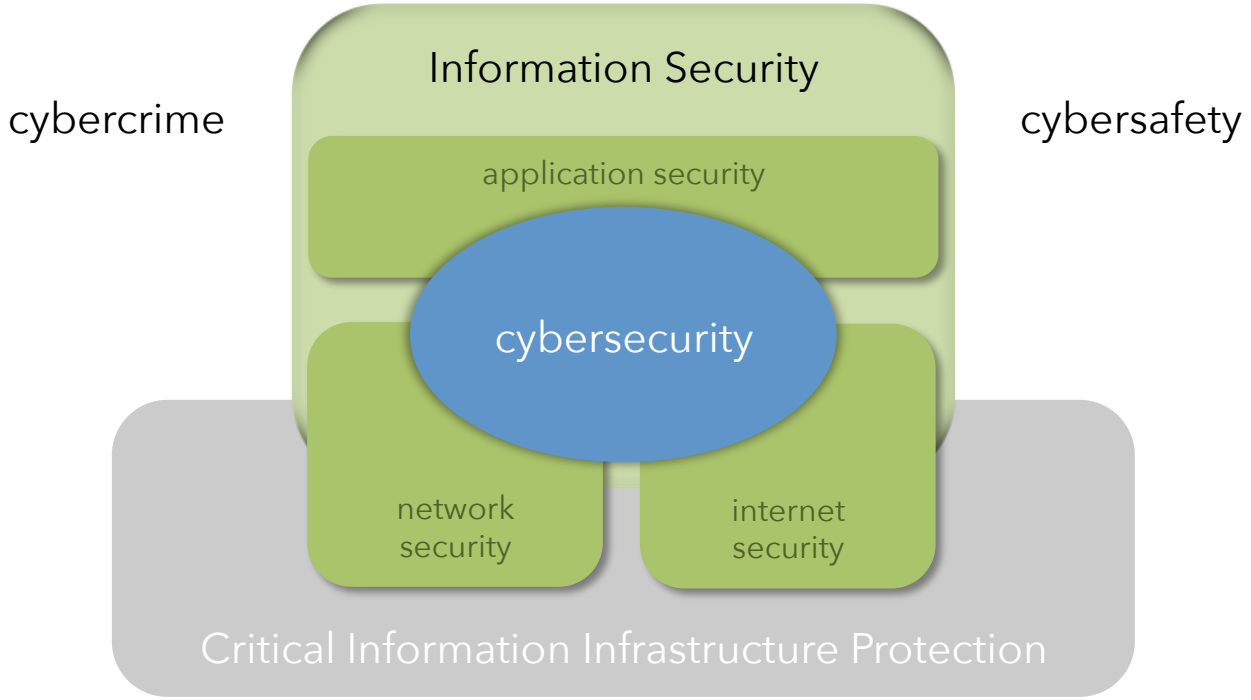
"domani"

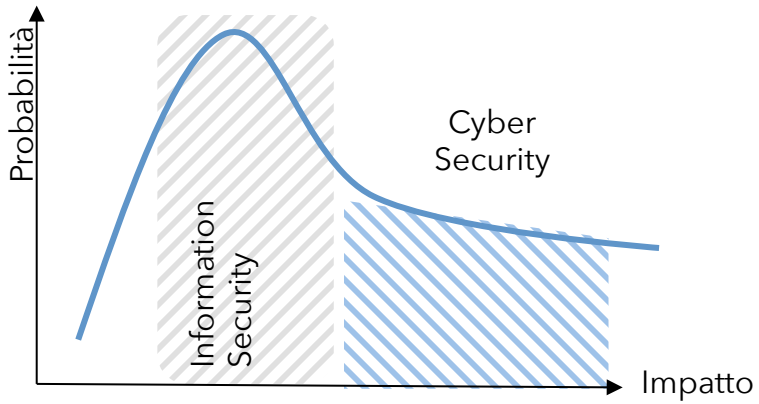
- Best Practices, standard di settore
- Minacce "invisibili"
- Metriche prospettiche



http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=296

Possiamo fare a meno dell'Information Security?





ISO 27032:2012

http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=296

Vantaggi della Cyber Security

Conoscere le minacce…

Per potersi focalizzare sulle contromisure!

- sono anch'esse note
- devo definire solo "l'intensità"

Break even della Cyber Security (dai limiti dell'Information Security…)

The **different focus** placed by each organization and provider in the Cyberspace on relevant security domains where **little or no input** is taken from another organization or provider **has resulted in a fragmented state of security for the Cyberspace**.

(ISO 27032:2012)

Aliena pericula, cautiones nostræ

- Information Sharing
  - Minacce, probabilità, soluzioni
- Valutazione del rischio e lesson learning: da dati interni a dati esterni
- Contromisure:
  - stesse soluzioni per problemi comuni
  - mediazione per obiettivi comuni
  - approccio coordinato

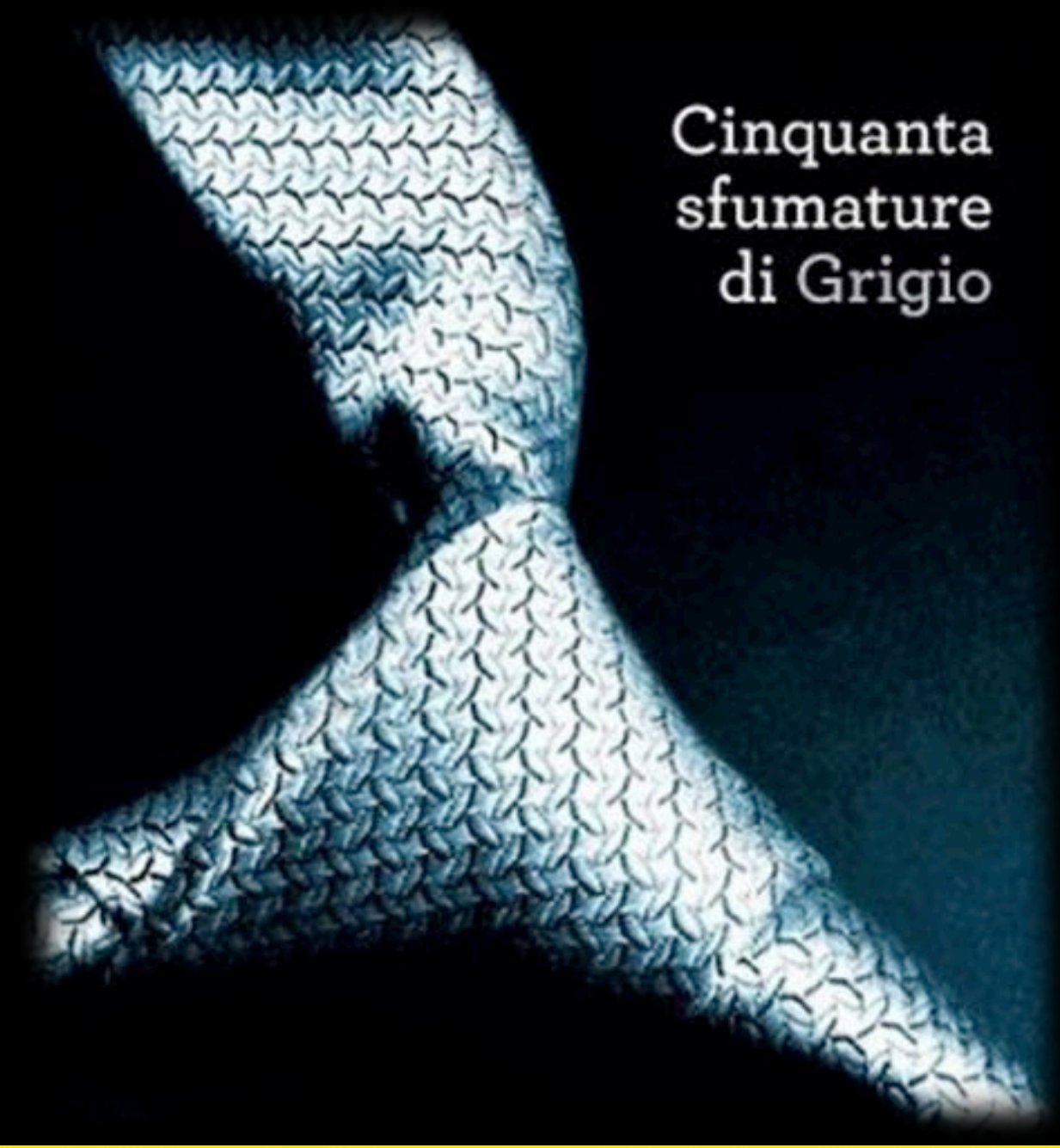
Information Security

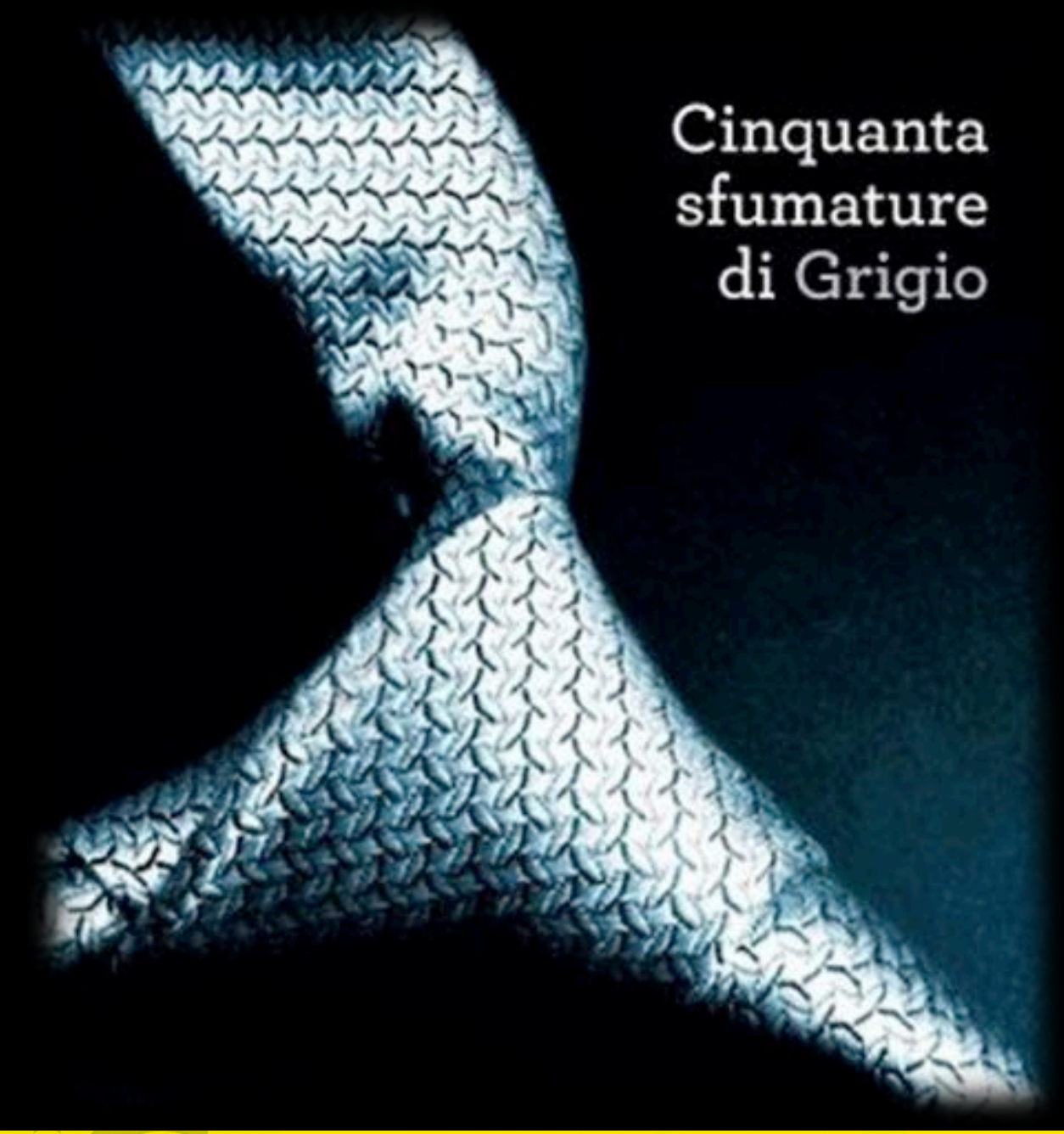
Contesto

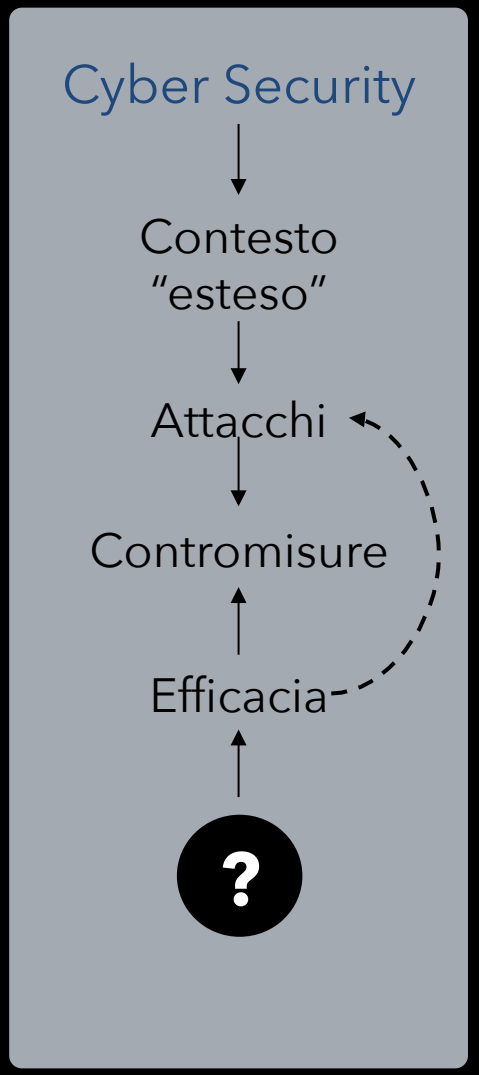
Rischi

Contromisure

Efficacia




Cinquanta
sfumature
di Grigio


Cyber Security
Contesto
"esteso"
Attacchi
Contromisure
Efficacia
?


Domande?