# Cybersecurity: rischi, contromisure e compliance

## Docenti: Barbara Indovina, Michele Slocovich

### Lingua

Italiano

### Descrizione del corso e obiettivi

Nell'era dell'interconnessione è sempre più difficile mettere al sicuro dati e informazioni. La trasformazione del modo di comunicare ha posto l'attenzione sulla necessità di proteggere adeguatamente i flussi di dati e i sistemi interconnessi. Al crescere della complessità delle architetture informatiche cresce da pari passo la complessità nel controllo manageriale sulle informazioni, sulle persone e sui mezzi predisposti per il loro trattamento. Le aziende sono esposte a gravi rischi spesso ignorati. Il corso vuole fornire agli studenti una panoramica sul contesto operativo della cyber security e sulla normativa Europea e Italiana relativa alla sicurezza dei dati e delle informazioni, fornendo gli strumenti necessari per comprendere le tecnologie ed il processo di governo della sicurezza e compliance aziendale alla normativa.

Gli obiettivi del corso sono di fornire agli studenti un approccio pratico e concreto al processo di governo e compliance all'IT security, partendo dai concetti di sicurezza dei dati e delle informazioni attraverso una lettura completa e critica delle normative in tema di sicurezza dei dati e del loro trattamento, senza tralasciare elementi di base per la comprensione degli aspetti tecnologici e di come questi possono (e devono) devono essere gestiti nelle organizzazioni.

Nell'ultima lezione del corso gli studenti parteciperanno all'analisi di un caso pratico di gestione di un incidente di sicurezza all'interno dell'azienda.

Alla fine del corso, i partecipanti saranno in grado di:

- Comprendere quali sono le principali minacce informatiche
- Comprendere come è possibile mitigare i rischi di un attacco informatico
- Comprendere le interdipendenze internazionali delle attività cyber
- Comprendere quali risorse aziendali sono necessarie nel processo di innalzamento del livello di sicurezza informatica
- Comprendere l'importanza della computer forensics per conservare adeguatamente le evidenze di un incidente informatico (Forensics Readiness)

## Destinatari

Il corso è aperto a tutti gli studenti Bocconi. In particolare si rivolge a tutti coloro che sono interessati a comprendere il contesto giuridico e tecnologico, le interazioni tra i due ambiti, e l'approccio in materia di compliance aziendale, sia dal punto di vista normativo che da quello tecnologico.

## Prerequisiti

Nessuno. Si consiglia tuttavia di aver superato un esame di informatica come Computer science o Informatica per giurisprudenza, o di possedere le competenze equivalenti.

## Regolamento

**Iscrizione:**
Le iscrizioni ai corsi possono essere effettuate esclusivamente tramite l'agenda dello studente yoU@B, nel box "Adesione attività varie".
È possibile annullare la propria iscrizione esclusivamente tramite agenda **entro e NON oltre** il termine delle iscrizioni al corso stesso. Non sono consentite altre modalità di cancellazione.
L'iscrizione verrà confermata qualche giorno prima dell'inizio del corso attraverso un messaggio nell'agenda yoU@B.

**Frequenza:**

- Frequenza pari o superiore al 75% delle lezioni: ottenimento dell'Open Badge
- Frequenza inferiore al 25% delle ore di lezione: inserimento in blacklist

## Modalità didattica

Sarà possibile partecipare al corso esclusivamente in maniera presenziale.

## Durata

12 ore

## Calendario

| Lezione | Data | Ora | Aula |
|---|---|---|---|
| 1 | lun 23/09//2024 | 18.15 - 19.45 | 203 (Sarfatti) |
| 2 | mer 25/09/2024 | 18.15 - 19.45 | 203 (Sarfatti) |
| 3 | lun 30/09/2024 | 18.15 - 19.45 | 203 (Sarfatti) |

| | | | |
|---|---|---|---|
| 4 | mer 02/10/2024 | 18.15 - 19.45 | 203 (Sarfatti) |
| 5 | mer 09/10/2024 | 18.15 - 19.45 | 203 (Sarfatti) |
| 6 | lun 14/10/2024 | 18.15 - 19.45 | 203 (Sarfatti) |

## Programma delle lezioni

| Lezione | Argomenti |
|---|---|
| 1 | **La sicurezza informatica**<br>- Definizioni<br>- Sicurezza dei dati, sicurezza delle informazioni<br>- La Cyber security come gestione del rischio<br>- Approccio e misura del rischio cyber |
| 2 | **La sicurezza in azienda**<br>- Compliance aziendale<br>- La normativa europea (ENISA, Direttive NIS)<br>- Information warfare (la guerra delle informazioni)<br>- Il GDPR<br>- Policy e procedure<br>- La gestione dell'incident (data breach)<br>- Esempi pratici: le CEO Fraud |
| 3 | **Il contesto: i come ed i perché degli attaccanti**<br>- Internet e protocolli<br>- Perché internet non è sicuro ?<br>- Modello perimetrale, modello aperto<br>- Autenticazione<br>- Uno schema per orientarsi<br>- Gli agenti e Le vulnerabilità |
| 4 | **Attacchi e prevenzioni**<br>- Misure Organizzative:<br>o Il fattore umano: Training, consapevolezza<br>o I ruoli aziendali coinvolti: DPO, CISO, CRO<br>- Identificazione del problema, intervento, ripristino, notifica del breach<br>- Unità di crisi multifunzionale<br>- Acquisizione forense delle evidenze, ripristino dei sistemi<br>- Digital Forensics: investigazione con valore probatorio delle risultanze<br>- Riferimenti normativi<br>- La Forensic Readiness |

| | |
|---|---|
| 5 | **Difesa – tecniche e strumenti**<br>- Misure Tecniche di difesa<br>o perimetrale, interna, preventiva, reattiva<br>o monitoraggio<br>- La kill chain<br>- La propagazione dei rischi<br>- I principali framework di riferimento per la Cyber security |
| 6 | **Analisi di un caso pratico**<br>- Partendo da casi di cyber attacchi realmente accaduti, verrà analizzata la gestione della cyber crisis sotto il profilo tecnico, legale ed organizzativo.<br>Attività di debriefing del caso e analisi delle possibili soluzioni |

## Bibliografia suggerita

Materiali prodotti dai docenti

## Posti disponibili

Questa attività è a numero chiuso quindi l'iscrizione non sarà possibile oltre **110 posti** o dopo la chiusura del periodo di iscrizione.
E' possibile annullare l'iscrizione esclusivamente tramite agenda yoU@B entro e NON oltre il termine delle iscrizioni al corso stesso