ACCADEMIA DEI SERVIZI PUBBLICI

Corso di Formazione on line

"Cyber Risk – Un approccio risk driven applicato al cyber e ingaggio più efficace del CdA e del top Management" *(COD.23.007)*

30 marzo 2023

Contesto

Il cyber risk non è solamente un tema per i "tecnici" del settore ma è un tema prioritario per il top management e parte integrante dell'agenda del CdA. La proliferazione delle tecnologie ha causato un aumento esponenziale della superficie di rischio e del volume delle minacce, anche il livello di sofisticazione degli attacchi è cresciuto, le aziende si trovano ad operare in un ecosistema sempre più aperto a terze parti con una value chain più complessa. Anche il fattore "umano" è molto rilevante, in molti casi gli attacchi sono perpetrati utilizzando tecniche di social engineering o phishing, sfruttando la scarsa consapevolezza degli utenti e/o falle nelle procedure. Il programma di cybersecurity non mette al riparo da qualsiasi minaccia, né consente di azzerarne i rischi, è fondamentale qualificare l'appetito al rischio cyber e quantificarne l'esposizione, analizzando gli scenari di attacco calandoli sulla realtà aziendale, anche per prioritizzare gli investimenti in protezione, ma soprattutto per settare correttamente le aspettative del CdA e del top management, impostando un dialogo orientato al rischio.

Obiettivi

- Proporre un approccio risk driven applicato al cyber: sistema di protezione sempre più su misura, basato sulla cybersecurity posture, sull'esposizione al rischio e sul cyber risk appetite, per un ingaggio più efficace del CdA e del top management

Destinatari

- Operatori Power & Gas, idrici e gestione dei rifiuti
- COO, CIO, CISO
- Resp. Enterprise Risk Management

Durata e luogo

Il corso si compone di una giornata formativa in video-conferenza con la piattaforma Zoom, secondo il programma dettagliato qui di seguito indicato; il link con password sarà fornito a tutti gli iscritti con mail individuale.

Programma dettagliato

Giovedì 30 marzo 9.30 – 13.30

- Evoluzione del contesto delle minacce dal punto di vista delle sfide sottostanti
- Le competenze chiave per la C-suite in ambito Cyber risk

Pausa caffè

- Come ingaggiare il CdA e il top Management in modo efficace sul Cyber risk
- Case study: quantificazione esposizione rischio Cyber di uno scenario di attacco

DOCENTI

Angelo Rosiello – Partner, Oliver Wyman

Laureato con lode in Ingegneria Informatica presso il Politecnico di Milano, ha completato il PLD (Program for Leadership Development) presso la Harvard Business School, e ha conseguito certificazioni ITIL e Scrum master.
Partner dell'ufficio di Milano, 16 anni di esperienza in consulenza strategica, con focus sulle Utility e competenze funzionali cross-industry nell'ambito della cybersecurity, dell'eccellenza operativa, Digital & innovation, IT & Analytics.
Tra le esperienze rilevanti in ambito cyber:

- Cyber risk management per una primaria banca italiana: progettata la nuova metodologia per quantificare (in euro) l'esposizione a diversi scenari cyber;
- Modello operativo di cybersecurity per una società oil&gas: progettato il modello operativo di sicurezza informatica (organizzazione, processi, capability, ecc.) applicabile all'intera azienda e definito un master plan per raggiungere il livello di sicurezza target;
- Cyber risk appetite per una primaria banca italiana: definito il risk appetite per l'ambito cyber, inclusi gli indicatori di monitoraggio.

Anna Maria Rosati – Principal (Director), Oliver Wyman

Laureata con lode in Ingegneria Informatica, Laurea Magistrale, presso il Politecnico di Milano, ha conseguito certificazioni ITIL e Scrum master, e completato corsi executive presso INSEAD e Wharton Business School.
Principal (Director) della practice Digital in Italia, 15 anni di esperienza in consulenza strategica, con competenze in ambito cyber, IT strategy & transformation, digital & innovation.
Tra le esperienze rilevanti in ambito cyber:

- Cyber risk management per una primaria banca italiana: progettata la nuova metodologia per quantificare (in euro) l'esposizione a diversi scenari cyber;
- Modello operativo di cybersecurity per una società oil&gas: progettato il modello operativo di sicurezza informatica (organizzazione, processi, capability, ecc.) applicabile all'intera azienda e definito un master plan per raggiungere il livello di sicurezza target;
- Benchmarking su cyber risk management nel settore bancario: condotto un benchmarking su istituti primari sui livelli di maturità delle capability e gap nella gestione del rischio cyber.