CURRICULUM VITAE
ET STUDIORUM

INFORMAZIONI PERSONALI

Nome	**GERARDO COSTABILE**
Indirizzo	**XXXXX**
Telefono	**+39.XXXXX**
E-mail	**gerardo@costabile.net**
Nazionalità	Italiana

ESPERIENZA LAVORATIVA

• Date (da – a)	Novembre 2016/oggi
• Datore di lavoro	CEO - Deepcyber srl
• Tipo di impiego	**Advanced Intelligence – Protection – Cyber Security – Antifraud**

• Date (da – a)	Da luglio 2016/ottobre 2016
• Datore di lavoro	British Telecom Italia – Roma
• Tipo di impiego	**Chief Security Officer e Country Leadership team per Italia ed Europa continentale (Italia, Spagna, Francia, Germania, Ungheria, Benelux)**

Budget: MLN di euro (dato confidenziale)

L'organizzazione, con 35 risorse in Italia e 25 all'estero, ha le seguenti strutture e competenze organizzative aziendali:

- Cyber Security e CSIRT
- Fraud Management (interne ed esterne)
- Intelligence e prestazioni di giustizia (tabulate, intercettazioni, etc)
- Physical security
- Data protection, risk security e compliance
- Commercial & contract security

• Date (da – a)	Da novembre 2015/luglio2016
• Datore di lavoro	Fastweb Spa (Swisscom AG Group) – Milano
• Tipo di impiego	**Chief Security Officer (Security & Safety)**

Budget: MLN di euro (dato confidenziale)

Il dipartimento, che consta di oltre 100 risorse tra interne ed esterne, ha le seguenti strutture e competenze organizzative aziendali:

- Intelligence & Lawful Interception
- Physical security
- Business & ICT Security

- Fraud management (corporate ed external revenue fraud)
- Security operation center (Corporate SOC)
- Relazioni con Law Enforcement, National Security Authority ed altre Authority (Privacy, Agcom, etc);
- Data protection, privacy
- Risk Security e corporate compliance
- Business continuity, disaster recovery e crisis management
- Safety
- Corporate social responsibility (GRI standard).
- Gestione delle certificazioni sull'information security (ISO 27001), business continuity management system (BS 25999/ISO 22301), ICT service management system (ISO 20000), quality management system (ISO 9001), environment management system (ISO 14001) ed health and safety management system (OHSAS 18001).

• Date (da – a)	Da giugno 2012/novembre2015
• Datore di lavoro	Ernst&Young – Roma, Milano
• Tipo di impiego	**Executive Director – Responsabile per l'Italia e per la Western Zone EMEIA (Italia, Spagna, Francia, Portogallo, Lussemburgo, Olanda, Belgio, Marocco, Algeria) della Business Unit denominata "Forensic Technology & Discovery Services", all'interno del Fraud Investigation & Dispute Services. Il ruolo ricoperto riporta, tra l'altro, al Partner responsabile per EMEIA (con sede a Londra) del Forensics Technology (approccio tipico matriciale).**

Il dirigente si occupa end to end con il suo team dell'offerta di business di EY (e relativa delivery progettuale) nei settori Fraud Audit, Anticorruzione, Cybercrime, Cybersecurity, IT Forensics, E-discovery, Intelligence, Fraud Data Analytics, Enterprise Fraud Management System; AntiMoneyLaudering, Compliance & Dispute per aziende principalmente Global Fortune 500.

Egli, oltre ad avere esperienza nella gestione di team e progetti complessi ed articolati all'interno di aziende di medio-grandi dimensioni, è altresì membro del tactical group worldwide di EY sul cybercrime/cybersecurity ed è responsabile dell'acquisition plan worldwide di boutique ICT del settore, da parte di EY Global.

Per progetti, opportunità e acquisizioni societarie, il dirigente intrattiene relazioni internazionali e viaggi di lavoro su UK, USA, Russia, Emirati Arabi oltre che nella propria zona EMEIA.

Le industry con maggiori esperienze sono Telecom, Financial Services, Banking, Credit Card, Gaming, Military, Oil & Gas, Gov.

• Date (da – a)	Da maggio 2006/Aprile 2012
• Datore di lavoro	Poste Italiane spa (www.poste.it) – Roma
• Tipo di impiego	**Dirigente – Chief Information Security Officer. Il ruolo ricoperto rispondeva al Senior Vice President Security & Safety, a riporto dell'Amministratore Delegato di Poste Italiane. La funzione era composta da 20 dipendenti, tra tecnici e legali, oltre ad numerosi consulenti e società esterne. Budget: MLN di euro (dato confidenziale).** I compiti principali erano i seguenti:

a) Infosec Risk Management, piano strategico e requisiti di sicurezza ICT e business security, con particolare riguardo alla mitigazione dei rischi di sicurezza informatica, frodi informatiche *et similia*. Ha partecipato, tra le iniziative più importanti, a definire la sicurezza informatica e le prestazioni obbligatorie di giustizia di Poste Mobile, il primo operatore di telefonia mobile che consente movimentazione di denaro tramite il cellulare.
b) Fraud management per frodi tecnologiche o supporto tecnologico per analisi dati, informazioni e innovazione in caso di frodi tradizionali.
c) Privacy/Data Protection Officer per il Gruppo Poste Italiane, con coordinamento di 350 dirigenti su tutto il territorio nazionale.
d) Sicurezza organizzativa: Security Policy, Standard e Linee Guida per tutto il Gruppo

Poste Italiane, in linea con le volontà del Top Management.

e) monitoraggio di II° livello, ovvero sull'attuazione e compliance alle Information Security Policy e Standard emesse.

f) sensibilizzazione, educazione, e comunicazione a livello di Gruppo su tematiche di Information Security, collaborando altresì alle attività relative alla *Cybersecurity & Electronic Crime Task Force.*

g) Presiedere il Comitato Operativo per la Sicurezza delle Informazioni, con le seguenti responsabilità:

- assicurare la predisposizione del Piano Strategico di Azione contenente gli interventi da realizzare nel medio-lungo termine con evidenza delle risorse necessarie;
- coordinare la gestione e il monitoraggio dei progetti più rilevanti, al fine di fornire regolare informativa al Comitato Guida relativamente al raggiungimento degli obiettivi e alle principali aree critiche;
- definire le modalità di implementazione del modello di governance attraverso il coordinamento delle attività operative.

g) sviluppo piattaforme ICT di settore, oltre che gestione come program/project manager degli sviluppi infrastrutturali tecnologici di Security & Safety di Gruppo (security rooms, antifraud solutions).

• Data (da – a)	Da dicembre 2010/ 2013
Nome e indirizzo del datore di lavoro	**Consortium GARR (*associazione senza fini di lucro fondata con il patrocinio del Ministero dell'Istruzione, dell'Università e della Ricerca, che gestisce la rete telematica italiana dell'Università e della Ricerca).*** Roma
• Tipo di impiego	**Membro del comitato Audit Sicurezza**

• Date (da – a)	Da 1997/2006
• Nome e indirizzo del datore di lavoro	Guardia di finanza
• Tipo di impiego	**Sottufficiale del Gruppo Repressione Frodi della Guardia di Finanza** di Milano. Indagini nel settore della corruzione, white collar crimes (anche nei confronti della pubblica amministrazione), antiriciclaggio, contrasto al terrorismo, nazionale e internazionale, a supporto principalmente della Procura della Repubblica di Milano.

Negli anni 2001-2006 ha attivato un team specializzato nella *computer forensics* e nel settore degli abusi tecnologici, quale esperto nella formazione e cristallizzazione della c.d. prova informatica. Coordinatore della prima indagine di phishing e cybericiclaggio in Italia (anno 2005), con arresti di cittadini dell'Est e con oltre 150 indagati.

Ha cooperato con Autorità governative, militari e di intelligence americane ed europee, quali ad esempio la NASA, l'US Army, l'US Navy, l'United States Secret Service e l'OLAF (Ufficio europeo per la lotta antifrode presso la Commissione Europea a Bruxelles) al fine di reprimere queste nuove forme di criminalità informatica transnazionale e frodi comunitarie.

Specializzato in intercettazioni telefoniche, telematiche, video, GPS e più in generale di tecnologia investigativa oltre che di sistemi di protezione e contrasto.

ESPERIENZA EXTRAPROFESSIONALE ED ASSOCIATIVA

Presidente dell'Italian e dell'European Chapter e Vicepresidente dell'International Chapter dell'IISFA (International Information Systems Forensics Association - www.iisfa.it), no profit Association. Il chapter italiano consta di 700 soci circa. Membro di numerose comunità di esperti di cybersecurity, cyber crime e digital investigation.

Membro permanente del **New York Electronic Crime Task Force** – team creato negli Stati Uniti dal Secret Service, con l'obiettivo di unire le competenze degli investigatori, esperti, accademici, grandi aziende, per il contrasto al cyber crime.

ISTRUZIONE E PERCORSO DI STUDI

• Date (da – a)	2011-2012
• Nome e tipo di istituto di istruzione o formazione	Executive MBA Business School "Luiss Guido Carli" – Roma
• Date (da – a)	2003 (durante il lavoro)
• Nome e tipo di istituto di istruzione o formazione	Laurea in economia e commercio - Tesi: Internet e la "vexata quaestio" del divieto delle aste on line - Alma Mater – Universtità di Bologna
• Date (da – a)	1993
• Nome e tipo di istituto di istruzione o formazione	Diploma superiore Liceo Scientifico Francesco Severi – Salerno

ALTRE DOCENZE

Professore a contratto all'Università di Foggia e all'Univ Telematica San Raffaele di Roma, già cultore della materia presso l'Università La Sapienza di Roma (in informatica forense), è stato docente presso la Scuola Superiore della Magistratura, il Consiglio Superiore della Magistratura e presso numerose Università, quali ad esempio quelle di Milano (Statale e Politecnico), Camerino, Roma (La Sapienza e LUMSA), Orvieto (Luiss), Potenza, Campobasso, Siena, European School of Economics (Milano) per master, cicli seminariali, conferenze e lezioni agli studenti, con temi afferenti la Privacy, criminalità informatica, cybersecurity, cyberintelligence, computer forensics, anticorruzione.

Dal 2000 al 2006, formatore interno della Guardia di finanza per corsi, training e convegni sull'informatica giuridica e giudiziaria, in particolare per la sicurezza informatica, la privacy, la computer forensics, intercettazioni telematiche.

Dal 2006 al 2012 formatore interno di circa 350 dirigenti di Poste Italiane (ogni anno), sui temi relativi alla privacy ed alla sicurezza delle informazioni.

PUBBLICAZIONI

Autore e coautore di numerose pubblicazioni e/o interviste (sia su stampa che in televisione). Si segnalano, in particolare, alcune delle maggiori pubblicazioni:

a) Gerardo Costabile (a cura di) SICUREZZA E PRIVACY: DALLA CARTA AI BIT - Manuale per aziende, studi professionali, pubblica amministrazione - ed. Experta 2005
b) AA.VV. Reati informatici e attività di indagine: dal cyberterrorismo alla computer forensics Ed. Experta 2007
c) F. Cajani - G. Costabile - G. Mazzaraco - Phishing e furto d'identita' digitale - Indagini informatiche e sicurezza bancaria. Prefazione di Giuseppe Corasaniti - Ed. Giuffrè 2008
d) Gerardo Costabile - INFORMATION SECURITY IN AZIENDA - Ed. experta 2008
e) Aterno - Cajani – Costabile – Mattiucci – Mazzaraco – Computer forensics ed indagini digitali (3 volumi, 2300 pagine) – Ed Experta 2011.
f) Gerardo Costabile, Antonino Attanasio, Mario Ianulardo - IISFA Memberbook 2019 DIGITAL FORENSICS: Condivisione della conoscenza tra i membri dell'IISFA ITALIAN CHAPTER
g) Gerardo Costabile, Antonino Attanasio, Mario Ianulardo - IISFA Memberbook 2018 DIGITAL FORENSICS: Condivisione della conoscenza tra i membri dell'IISFA ITALIAN CHAPTER
h) Gerardo Costabile, Antonino Attanasio, Mario Ianulardo - IISFA Memberbook 2017 DIGITAL FORENSICS: Condivisione della conoscenza tra i membri dell'IISFA ITALIAN CHAPTER
i) Gerardo Costabile, Antonino Attanasio, Mario Ianulardo - IISFA Memberbook 2016 DIGITAL FORENSICS: Condivisione della conoscenza tra i membri dell'IISFA ITALIAN CHAPTER
l) Gerardo Costabile, Antonino Attanasio, Mario Ianulardo - IISFA Memberbook 2015 DIGITAL FORENSICS: Condivisione della conoscenza tra i membri dell'IISFA ITALIAN CHAPTER
m) Gerardo Costabile, Antonino Attanasio, Mario Ianulardo - IISFA Memberbook 2014 DIGITAL FORENSICS: Condivisione della conoscenza tra i membri dell'IISFA ITALIAN CHAPTER
n) Gerardo Costabile, Antonino Attanasio, Mario Ianulardo - IISFA Memberbook 2013 DIGITAL FORENSICS: Condivisione della conoscenza tra i membri dell'IISFA ITALIAN CHAPTER
o) Gerardo Costabile, Antonino Attanasio, Mario Ianulardo - IISFA Memberbook 2012 DIGITAL FORENSICS: Condivisione della conoscenza tra i membri dell'IISFA ITALIAN CHAPTER
p) Gerardo Costabile, Antonino Attanasio, Mario Ianulardo - IISFA Memberbook 2011 DIGITAL FORENSICS: Condivisione della conoscenza tra i membri dell'IISFA ITALIAN CHAPTER
q) Gerardo Costabile, Antonino Attanasio, Mario Ianulardo - IISFA Memberbook 2010 DIGITAL FORENSICS: Condivisione della conoscenza tra i membri dell'IISFA ITALIAN CHAPTER
r) Gerardo Costabile, Antonino Attanasio, Mario Ianulardo - IISFA Memberbook 2009 DIGITAL FORENSICS: Condivisione della conoscenza tra i membri dell'IISFA ITALIAN CHAPTER
s) F. Cajani, G. Cernuto, G. Costabile, F. D'Arcangelo - Le nuove frontiere dell'acquisizione degli elementi di prova nel cyberspace.
t) Gerardo Costabile, Ilenia Mercuri, Il fattore umano nella cybersecurity: Phishing, Social Engineering e Mind Hacking, Amazon ed, 2018

LINGUE STRANIERE

Inglese: Fluente (scritto e parlato, per lavoro)

CAPACITÀ E COMPETENZE RELAZIONALI

Comunicazione (anche in pubblico) e relazioni personali. Correttezza nelle relazioni personali e professionali. Gestione dei collaboratori, team building, change management anche in ambiente multiculturale e multinazionale.

CAPACITÀ E COMPETENZE ORGANIZZATIVE

Attento alla gestione ed al coaching dei collaboratori - anche in ambiente particolarmente competitivo o da "start up organizzativo" -, al problem solving ed alla visione d'insieme, ama guidare con l'esempio e con le competenze. Innovazione, iniziativa, motivazione, determinazione, perseveranza, entusiasmo e passione nell'innovazione e nel raggiungimento degli obiettivi.

CAPACITÀ E COMPETENZE TECNICHE CERTIFICAZIONI

Certified Information Forensics Investigator **(CIFI),** Certified in the Governance of Enterprise IT **(CGEIT),** Certified in Risk and Information Systems Control **(CRISC),** Certified Hacking Forensics Investigation **(CHFI)** e AccessData Certified Examiner **(ACE)** riconosciute in ambito internazionale e conseguite rispettivamente presso l'IISFA International (www.iisfa.org), EC-Council, ISACA (www.isaca.org) ed Accessdata.