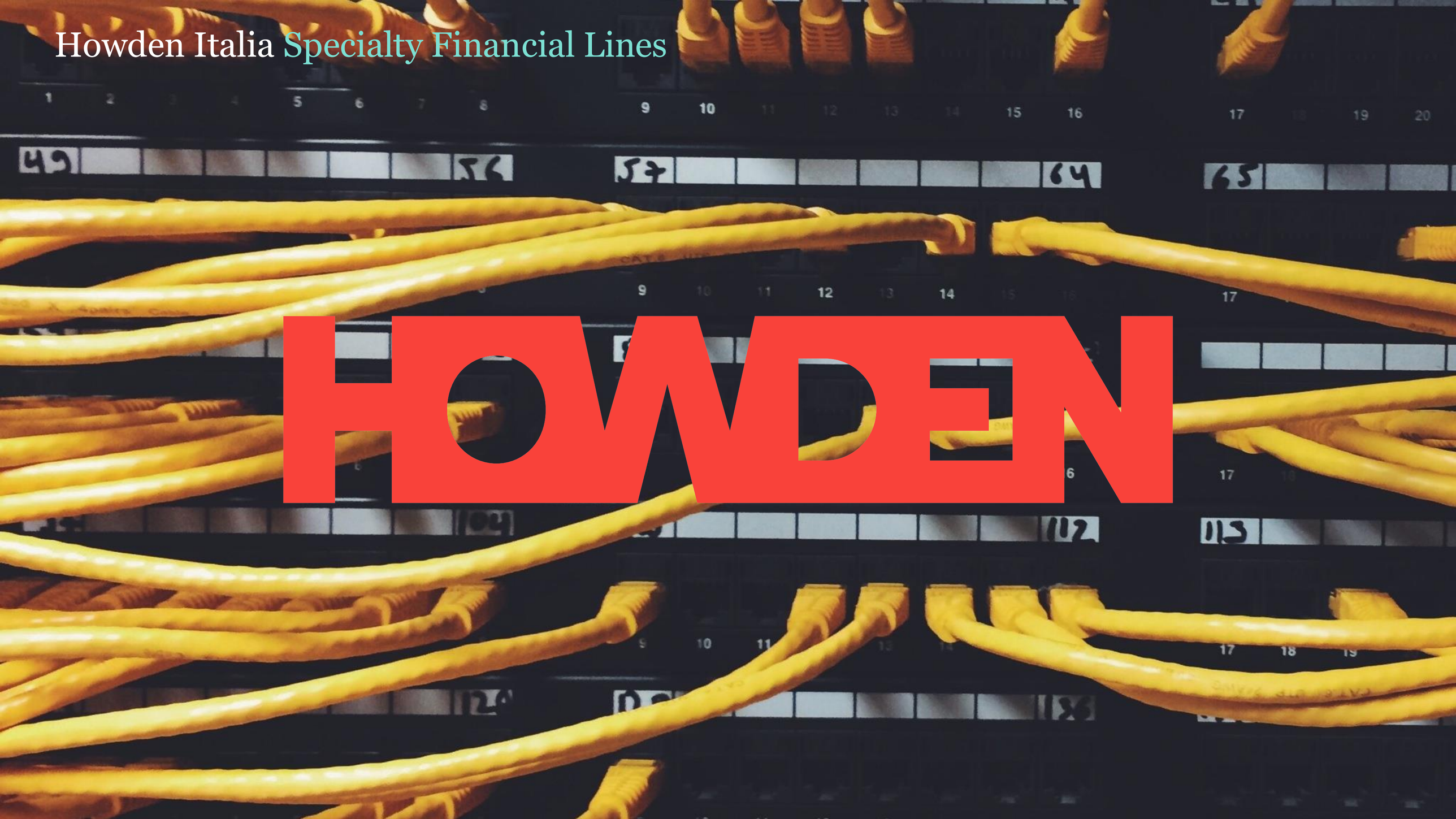
Howden Italia Specialty Financial Lines



Polizza Cyber

Trasferimento al mercato assicurativo del rischio cyber

Specialty Financial Lines

2024

HOWDEN

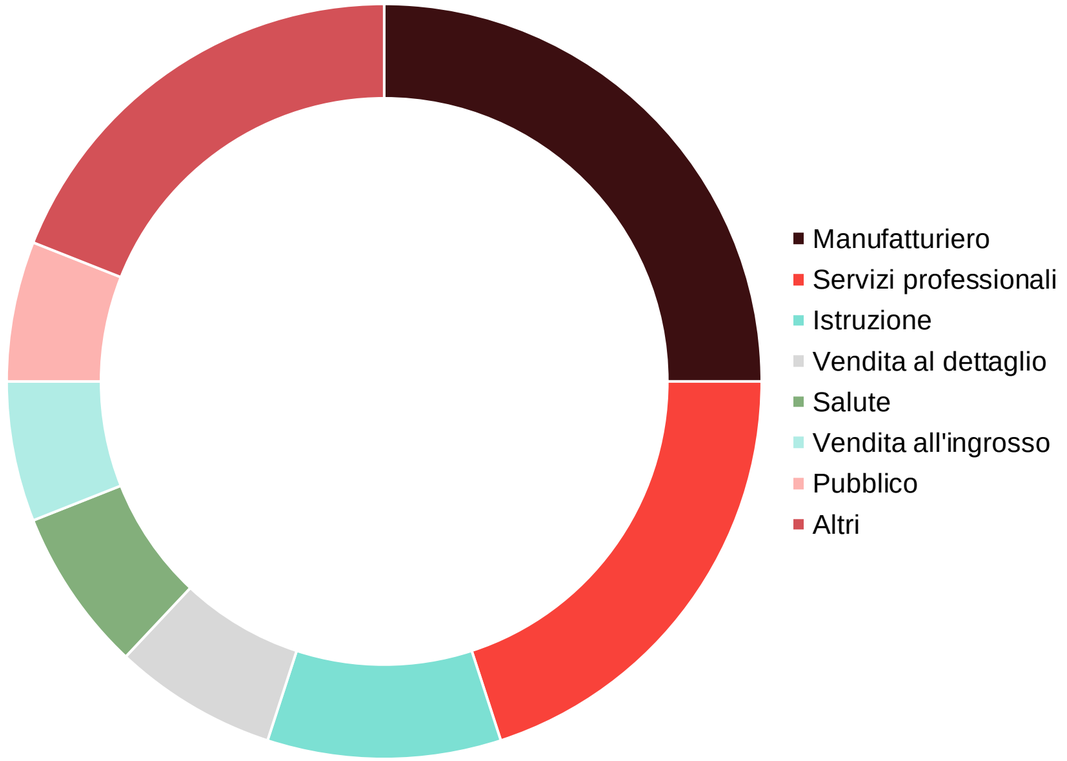
Andamento del mercato Cyber in Europa nel 2023

Nel 2023 la cyber security deve essere una priorità assoluta per le aziende. Con le minacce che diventano sempre più sofisticate e le aziende che diventano sempre più dipendenti dalle tecnologie digitali, è fondamentale garantire che le informazioni e i dati siano protetti in modo efficace.

Il Q2 ha visto un aumento significativo degli attacchi ransomware: la frequenza è aumentata di quasi il 50% rispetto al corrispondente periodo del 2022. A rivelarlo è il terzo report annuale sugli andamenti della cyber insurance a firma Howden. Secondo lo studio, il mercato assicurativo cyber globale potrebbe raggiungere i 50 miliardi di dollari entro il 2030 e le aziende più colpite sono proprio quelle manufatturiere.

Possiamo ritenere attenuta la fase di hard market: il mercato assicurativo ha interesse ad assicurarsi che le aziende abbiano investito in misure proattive di gestione del rischio e cybersecurity per ridurre la probabilità e l'impatto di una perdita. Mentre per alcune PMI può essere difficile identificare e prevenire i rischi informatici, buoni profili di rischio generano appetito da parte degli assicuratori, portando migliori quotazioni.

Settori più colpiti dagli incidenti cyber



Howden Italia Specialty Financial Lines

Trasferimento al mercato assicurativo del rischio cyber

Polizza Cyber

Copertura danni propri

COSTI E SPESE

- Interruzione dell'attività
- Estorsione Cyber
- Ripristino dei dati e dei sistemi
- Costi di difesa risultanti da un'indagine regolamentare

INCIDENT RESPONSE

- Call center per supporto 24/7
- Specialisti per la negoziazione del ransom
- Consulenti per attività di Forensic
- Crisis Communications Experts - PR

Copertura R.C. verso Terzi

CONTENZIOSI

- Richieste di risarcimento da parte di Terzi conseguenti a una Violazione della sicurezza
- Richieste di risarcimento da parte di Terzi conseguenti ad una Violazione delle informazioni e dei dati confidenziali

RESPONSABILITÀ CIVILE

- Responsabilità derivante dai Media

Sezione Danni Propri (1/2)

Perdite dirette, costi e spese sostenuti dall'Assicurato

	DESCRIZIONE	COSTI COPERTI
Interruzione dell'attività	Si intende la sospensione, carenza, peggioramento e/o ritardo, effettivi e misurabili, delle prestazioni del sistema informatico dell'assicurato per effetto di un evento assicurato.	• Perdita di profitto lordo; oppure in alternativa • Aumento del costo del lavoro
Costi e spese	Ripristino e backup dei dati e degli altri asset digitali che sono stati danneggiati o distrutti a seguito di una Violazione della sicurezza.	• Costi di mitigazione e di bonifica dei sistemi • Costi per ripristinare il sistema informatico dell'Assicurato • Costi per mantenere attivo il sistema informatico dell'Assicurato • Digital Forensics
Protezione dei dati personali	Contravvenzione ad obblighi legali e normativi derivanti da una Violazione delle informazioni e dei dati confidenziali («data breach»).	• Costi di difesa (procedimento penale o indagine dell'Autorità Garante) • Costi di mitigazione • Costi per definire una strategia volta a limitare un danno reputazionale all'Assicurato
Sanzioni / Indagini di Autorità	Sanzioni imposte da un'autorità di regolamentazione come risultato di un'indagine.	• Costi di difesa sostenuti dall'Assicurato come risultato di un'indagine effettuata da un'Autorità di regolamentazione • È escluso il pagamento di tasse, multe e sanzioni imposte dall'Autorità di regolamentazione

Sezione Danni Propri (2/2)

Perdite dirette, costi e spese sostenuti dall'Assicurato

	DESCRIZIONE	COSTI COPERTI
Cyber estorsione	Estorsione informatica (**Ransomware**) con minaccia della perdita e/o pubblicazione di dati.	• Costi per esperti nella negoziazione del riscatto • Qualora ammesso dall'assicuratore, indennizzo del pagamento del riscatto
Consulente esterno	Qualsiasi persona fisica o giuridica nominata direttamente dagli assicuratori al fine di ottenere supporto specializzato e competente nella gestione dell'evento assicurato.	• Costi dei consulenti incaricati (attenzione alla sovrapposizione di ruoli)
Strategia di comunicazione	Costi e spese per definire e/ o implementare una strategia di comunicazione volta a limitare qualsiasi danno alla reputazione dell'Assicurato.	• Costi per mitigare il danno reputazionale (es. costi di agenzia di comunicazione)

Sezione Responsabilità Civile Cyber

Costi per danni causati a Terzi derivanti dalla responsabilità dell'Assicurato a seguito di un incidente informatico

	DESCRIZIONE	COSTI COPERTI
Violazione delle informazioni e dei dati confidenziali	Esfiltrazione e divulgazione di dati derivante da un accesso non autorizzato ai sistemi informatici dell'Assicurato che determina una violazione della privacy.	• Costi di difesa • Danni derivanti da una richiesta di risarcimento di un Terzo a seguito di una violazione della confidenzialità dei dati personali
Violazione della sicurezza	Violazione dei sistemi informatici che porta all'accesso non autorizzato ai dati di un computer, ad applicazioni, a reti o dispositivi. La violazione potrebbe essere riconducibile all'inosservanza di misure volte a prevenire o mitigare un attacco cyber.	• Costi di difesa • Danni derivanti da una richiesta di risarcimento di un Terzo a seguito di una violazione della sicurezza
Responsabilità derivante dai Media	Responsabilità derivante da (i) diffamazione, calunnia o danno alla reputazione di una persona fisica o giuridica; (ii) violazione di qualsiasi diritto sulla proprietà intellettuale, copyright, slogan, marchio commerciale, ditta, licenza, brevetto, idea, informazione, informazione o nome del dominio; (iii) violazione della privacy e/o diritto di immagine; (iv) furto d'identità.	• Costi di difesa • Danni derivanti da una richiesta di risarcimento di un Terzo come risultato di una qualsiasi riproduzione, pubblicazione, comunicazione, informazione o contenuto digitale pubblicato sul sito internet dell'Assicurato e/o sui siti di social networking

Requisiti fondamentali in ambito cybersecurity (1/2)

Trasferimento al mercato assicurativo del rischio cyber

I più attenzionati dai mercati assicurativi

Multi-factor Authentication

- Per l'accesso remoto
- Per le risorse cloud
- Per tutti gli utenti amministratori della rete interna

Endpoint Detection & Response

- Adozione di misure di sicurezza per prevenire o rilevare attività dannose.
- Esempi: Endpoint Protection Platform (EPP), Managed Detetcion and Response (MDR), Network Detection and Response (NDR) e SIEM

Backup

- MFA richiesto per l'accesso
- Backup offline
- Crittografia dei backup
- Test regolari di ripristino dei backup

Segmentazione

- Segmentare il più possibile tra funzioni, aree geografiche, reti guest, ecc.
- Segmentazione IT e OT

Management degli accessi privilegiati

- Account privilegiati gestiti con uno strumento PAM o una workstation ad accesso privilegiato (PAW)
- Software di gestione delle password per i dipendenti

Security Operations Center

- 24/7, 365 giorni
- Interno o gestito da terzi

Asset Management

- Routine di patching efficaci
- Inventario degli asset hardware e software in base agli strumenti
- Rilevamento di hardware non autorizzato

E-mail Security

- Funzionalità di screening
- Servizio di quarantena
- Etichettatura delle e-mail esterne
- DKIM, SPF or DMARC

Fortemente desiderato Preferibile

Requisiti fondamentali in ambito cybersecurity (2/2)

Trasferimento al mercato assicurativo del rischio cyber

I più attenzionati dai mercati assicurativi

Vulnerability Management

- Linea di base resistente
- Elevata copertura dei vulnerability scans
- Penetration test

Business Continuity

- Test di ripristino dei backup
- Piano di ripristino di emergenza o BCP

Operational Technology

- Segmentazione e gestione delle piattaforme legacy e non supportate nell'ambiente OT
- Funzionalità di protezione e scansione delle vulnerabilità

End of Life Software

- Routine di gestione del ciclo di vita
- Segmentazione
- Supporto esteso
- Fasi di mitigazione del rischio

Formazione

- Formazione annuale per sensibilizzare i dipendenti
- Simulazioni di phishing

Service Accounts

- Nessun account di servizio nel gruppo di amministratori del dominio
- Principio del minimo privilegio
- Rotazione delle password e strumenti

Procedure e best practice

- Politica sulla privacy
- Politica di classificazione dei dati

Informazioni personali

- Crittografia
- Ubicazione e segmentazione dello storage
- Gestione degli accessi

Fortemente desiderato Preferibile

Howden Specialty Financial Lines

Trasferimento al mercato assicurativo del rischio cyber

Il team e contatti

La Specialty Financial Lines di Howden conta 7 specialisti e si è dotata di un team di esperti in materia Cyber con l'obiettivo di fornire soluzioni strategiche, personalizzate ed innovative.

Roberto Panzeri

Specialty Director, Financial Lines

M: +39 345 1091545

E: roberto.panzeri@howdengroup.com

Anthea Vasta

Specialty Manager, Financial Lines

M +39 347 3090239

E: anthea.vasta@howdengroup.com

Luca Albertini

Specialty Manager, Financial Lines

M +39 366 6678609

E: luca.albertini@howdengroup.com

Francesco Brunetti

Cyber Practice Leader, Financial Lines

M +39 342 3836025

E: francesco.brunetti@howdengroup.com

Serena Calzone

Cyber Specialist, Financial Lines

M +39 348 344 5171

E: serena.calzone@howdengroup.com

Howden Italia

Chi siamo

Il Gruppo Howden è leader europeo di brokeraggio assicurativo. Operiamo in tutto il mondo con professionisti di talento che hanno l'esperienza necessaria per garantire il miglior servizio. Ci prendiamo cura di ogni singolo cliente, grande o piccolo che sia, perché lavoriamo con un obiettivo a lungo termine: costruire una realtà di cui essere orgogliosi.

Grazie al nostro modello aziendale unico, in cui i dipendenti sono il principale azionista, e alla cultura che ne deriva, possiamo contare sui migliori esperti del settore. Qualunque sia la vostra esigenza, a prescindere dalla complessità della sfida o dall'unicità della situazione, abbiamo le persone giuste capaci di creare la soluzione ottimale.

Facciamo assicurazione in modo diverso e siamo determinati a renderla migliore. Conosciamo a fondo il mercato e stiamo usando le nostre competenze per trasformarla in uno strumento per il benessere sociale.

I nostri clienti

- Aziende locali e internazionali
- Enti pubblici
- Professionisti
- Gruppi omogenei di acquisto
- Privati

howdengroup.com