**Slide 2.**

Cominciamo dall’articolo 41 della Costituzione italiana.

*“L’iniziativa economica privata è libera. Non può svolgersi in contrasto con l’utilità sociale o in modo da recare danno alla sicurezza, alla libertà, alla dignità umana. La legge determina i programmi e i controlli opportuni perché l’attività economica pubblica e privata possa essere indirizzata e coordinata a fini sociali.”*

In questo articolo costituzionale ritroviamo implicitamente il concetto di mutualità, di cui abbiamo già parlato ampiamente, e quello di sostenibilità, che affronteremo tra poco. Ci ricorda come qualunque impresa abbia in qualche modo a che fare con gli altri, con la società, e come quindi funzioni meglio rispettando i principi mutualistici. La sostenibilità, invece, garantisce la fattibilità nel tempo, la stabilità.

**Slide 3, 4 e 5.**

Il Codice civile (articolo 2082) ci viene in aiuto sul concetto di imprenditore. Imprenditore è chi esercita professionalmente un’attività economica organizzata al fine della produzione o dello scambio di beni o di servizi. Imprenditore è colui che sa assumersi rischi, dopo averli ben valutati e aver preso le misure necessarie a limitarne i danni. Ogni sua decisione è in qualche modo rischiosa: la sfida è appunto avviare, gestire e portare al successo un’attività imprenditoriale.

Il rischio più evidente è quello di perdere il proprio investimento: in denaro, in tempo, in reputazione, in aspettative, in energie personali. Avviare un’impresa richiede capitali, propri o prestiti, che finanzino i beni necessari (dai macchinari alla strumentazione informatica, dai locali per uffici e magazzini ai mezzi di trasporto, dalle reti di relazioni commerciali alla capacità di un marketing efficace). Ecco perché il profitto rappresenta la remunerazione di questo rischio.

**Slide 6 e 7.**

Dobbiamo ora dividere i rischi in due grandi categorie: i rischi imprenditoriali e i rischi puri.

I rischi imprenditoriali sono appunto quelli fisiologici del fare impresa: collegati ad eventi che possono produrre o perdite o guadagni, quindi se ben gestiti possono essere addirittura strategici (es. apro un pub in una zona dove non ce sono altri: il rischio è che in quella zona non ce ne sia la necessità, ma se prima ho indagato sulle motivazioni per cui in quel momento non ce ne sono altri e ne ho tratto conclusioni positive per la mia iniziativa, potrò sfruttare il fatto di non avere concorrenza!)

I rischi puri, detti anche “cattivi” sono quelli i cui eventi collegati possono portare unicamente conseguenze negative, perdite più o meno gravi (es. un incendio, un furto…)

I rischi imprenditoriali si dividono in: finanziari (investimenti sul mercato che possono andare bene o male a seconda anche delle azioni sui prezzi di molti operatori), industriali (legati all’attività produttiva, commerciale e amministrativa) dell’impresa e strategici (ricordiamo l’esempio precedente del pub).

**Slide 8 e 9.**

Consideriamo alcuni esempi di sfide perse da imprese famose.

Errore di leadership: l’allontanamento del fondatore di Apple, deciso dall’allora CEO John Sculley perché il rischio era la completa sovrapposizione dell’uomo con il marchio, non permetterà di guidare la società come durante i fasti degli esordi, e renderà necessario richiamare Steve Jobs, ovviamente offrendogli un compenso ancora più alto. Probabilmente l’intuizione di Sculley non era sbagliata in sé ma nella tempistica!

Errore sul rinnovamento tecnologico: Polaroid e Kodak negli anni ‘80 decisero di trascurare l’avvento della fotografia digitale, ritenendo che quel tipo di tecnologia non sarebbe stato economicamente accessibile alle masse ancora per molto tempo; si sbagliarono perché invece avvenne il contrario (oltre allo strumento che entrerà sul mercato con modelli economici, anche il fare fotografie diventerà meno oneroso non dovendo più acquistare i rullini e le stampe); la scelta causò il temporaneo fallimento dei due marchi.

Errore di mercato: Buzz, un social network creato da Google, nato per rispondere allo strapotere di Facebook, si rivelerà un fallimento perché contraddiceva il principio stesso che aveva dato il successo al concorrente (Facebook nasceva con lo scopo di far ritrovare amici “perduti”, quindi aveva senso iscriversi tutti allo stesso social per ritrovarli); successivamente nasceranno molti social diversificati, probabilmente anche Buzz sbagliò i tempi!

Danni da nuovi competitor: Blockbuster (noleggiava film, videogiochi, e simili), con 60 milioni di soci, punti vendita in 25 paesi, 4800 negozi solo negli Stati Uniti, si trovò ad essere vittima, come prima il cinema a causa sua, di un medium concorrente - internet - che forniva gli stessi prodotti ancor più comodamente e in apparenza più economicamente rispetto ad esso.

Errore da previsione di evoluzione del prodotto: Nokia, la cui crisi è corrisposta con l’esplosione sul mercato degli smartphone (dal 2007 in poi) a cui la società finlandese non aveva inizialmente saputo rispondere in maniera adeguata, continuando a produrre un telefono solido e con poche funzioni (anche qui avevano pensato che i tempi per l’accessibilità di massa agli smartphone fossero ancora lontani; avevano inoltre sottovalutato l’esigenza del consumatore ad avere un

prodotto che si rompa per poter acquistare il modello anche di poco tecnologicamente più nuovo!)

I rischi imprenditoriali non sono assicurabili: non si può scaricare su altri o condividere il rischio di perdite e non anche quello delle “vincite”!

**Slide dalla 10 alla 14.**

L’iniziativa d’impresa non può più prescindere dal concetto di sostenibilità. Ormai è evidente come tutto ciò che viene considerato solido, duraturo, passi da questo ampio concetto. La sostenibilità richiede una costante attenzione sui fronti: economico, sociale e ambientale. Ad esempio un prodotto è economicamente sostenibile se i suoi costi di produzione sono tali da garantire un prezzo finale di vendita accessibile; è socialmente sostenibile se per produrlo non vi è stato sfruttamento del lavoro; è ambientalmente sostenibile se durante la produzione o lo smaltimento non ha interagito in modo tossico con la natura.

Ogni anno consumiamo molte più risorse di quante la terra sia in grado di rigenerare e sprechiamo un terzo del cibo prodotto. Pratiche imprenditoriali sostenibili creano un circolo virtuoso tra imprese, fornitori, clienti…che a sua volta influisce positivamente sui cambiamenti climatici, che stanno avendo un’influenza via via maggiore sulle azioni umane.

I cambiamenti climatici stanno aumentando per frequenza e intensità, creando così nuovi bisogni di protezione dall’aleatorio. Questo ha fatto sì che le compagnie di assicurazione si predisponessero ad analisi personalizzate per imprese e famiglie, in modo da proporre un pacchetto di coperture il più efficiente possibile. Consigliamo di visitare il sito [www.derris.eu](http://www.derris.eu/) per maggiori approfondimenti e per simulazioni di ipotetici piani di rischio personalizzati per le imprese.

**Slide 15**

I rischi puri sono quelli da controllare, da arginare e si dividono in rischi: di beni (sui fattori produttivi materiali e della continuità produttiva), di responsabilità civile (si riferisce alle conseguenze dannose che l’attività può avere nei confronti di terzi: ad esempio, uno sbaglio dei dipendenti, un danno procurato da un prodotto difettato, un imprevisto prodotto dal fabbricato), di persone (alla forza lavoro possono accadere infortuni, malattia o morte).

Alla **slide 16** trovate una tabella sulle tipologie di rischio a cui attingere per esercitarvi tra poco nella redazione di un piano di rischio.

**Slide da 17 a 20.**

Il Cyber Risk. Nasce dalla enorme quantità di dati disponibili e di interconnessioni tra sistemi e device ed è il rischio operativo relativo alle informazioni, ai dati e agli asset tecnologici, con conseguenze in ordine a: riservatezza, disponibilità e integrità delle informazioni o dei sistemi informativi.

Un po’ di terminologia per capirci meglio.

L’Information Technology Asset èil complesso delle informazioni, dei software o hardware di proprietà di un’organizzazione che vengono adoperati nel corso delle attività di business.

L’impianto o sistema di elaborazione dati èla totalità delle apparecchiature elettroniche (unità centrali, periferiche, apparecchiature di servizio), elettricamente coordinate, necessaria per l’espletamento delle funzioni di elaborazione.

I Dati sonol’insieme di informazioni logicamente strutturate, elaborabili a mezzo di programmi.

Il Sistema informativo è quel complesso di elementi che rileva in modo sistematico e organizzato i fenomeni economici di interesse dell'azienda, nell’intento di rappresentarli in modo organico, utilizzando la tecnologia più appropriata.

La percezione del Cyber risk è ancora bassa, nonostante la relativa semplicità di attuazione di un attacco informatico e la Cyber dipendenza.

Ma subire un attacco informatico avrebbe ripercussioni: economiche (risarcire i clienti i cui dati sono compromessi; discesa delle quotazioni dell’azienda, che si deve fermare almeno in parte); relative all’emergenza nella gestione dei sistemi informatici (riuscire ad affrontare l’emergenza senza interrompere la normale attività? Si è trattato di una fuga di informazioni o di una perdita di dati, oppure di un attacco hacker? In che modo i dati sono stati smarriti o sottratti? Dove si trovano ora le informazioni? Sarà necessario spegnere il server o sostituirne il software? È stato messo a punto un piano per il ripristino dei servizi informatici? La risposta a tutte queste domande è cruciale e complessa). Inoltre vi è la gestione delle pubbliche relazioni, fondamentale per riconquistare la fiducia e tutelare la reputazione.

**Slide dalla 21 alla 24.**

Le tecniche di trattamento del rischio sono volte a ridurre i rischi (cioè intervenire sulle due dimensioni che lo definiscono, frequenza e gravità) o ad attenuare l’impatto economico-finanziario dei loro effetti (ovvero creare le premesse affinché, al verificarsi dell’evento, risulti ridotta l’incidenza economico-finanziaria della perdita che esso comporta).

Con la tecnica del trasferimento assicurativo si mettono in comune gli eventi sfavorevoli e si ripartiscono le loro conseguenze all’interno della collettività partecipante alla messa in comune. Ecco di nuovo comparire il concetto di mutualità.

Nel trattamento del rischio puro, le coperture dell’assicurazione possono riguardare:

* Perdite per danni alle persone o ai beni
* Responsabilità (liti promosse dai clienti, dipendenti, terzi)
* Interruzione di attività (perdita di profitti e altre perdite consequenziali)

Le condizioni generali di contratto estendono il risarcimento ai danni materiali direttamente causati dagli eventi e non ai danni indiretti. Tale copertura aggiuntiva può tuttavia essere ottenuta pagando un premio aggiuntivo o con l’inserimento di una clausola particolare nella polizza o stipulando un contratto a parte, legato a quello principale.

Il danno all’organizzazioneconsiste in danni materiali diretti (la distruzione o deterioramento di cose), in perdite patrimoniali indirette (costituiscono un pregiudizio economico non immediatamente conseguente a danni corporali o danni materiali, ma verso software e dati), in costi per la gestione della crisi.

Il danno cagionato a terzi potrebbe essere relativo a danni materiali, danni alla persona e perdite patrimoniali.

Per quanto riguarda le coperture dell’assicurazione sul Cyber risk, i danni indennizzabili direttamente o indirettamente sono causati da: furto, frode, privacy, manomissione dati***.***

**Slide da 25 a 27.**

Il problema di uno stato di crisi in un’impresa è duplice: l’entità e la durata della crisi.

Perdite ingenti per un’impresa sono un grosso ostacolo alla continuità e alla salubrità dell’impresa stessa, ma spesso il fattore cruciale è il tempo.

Ad esempio, se l’impresa è una compagnia telefonica e subisce un danno a uno dei ripetitori principali, ovviamente dovrà sostenere tutte le spese per il ripristino del servizio, ma dovrà farlo anche il più velocemente possibile, altrimenti i clienti migreranno verso un’altra compagnia (non potendo rimanere a lungo senza il servizio) e quasi sicuramente non torneranno indietro a crisi risolta (esistono molti sostituti simili, la crisi ha generato un danno e soprattutto sfiducia). Il danno maggiore all’impresa non è l’esborso pur ingente per la riparazione, ma la perdita dei clienti e di una buona reputazione sulla propria affidabilità.

Redigere un buon piano di rischio, o Disaster Recovery Plan, serve a limitare tutti i tipi di conseguenze dei rischi. Segue il flusso temporale del verificarsi di un evento dannoso: prima deve analizzare i rischi e formulare ipotesi su ciò che potrebbe accadere, durante deve saper gestire la crisi tramite un piano di emergenza, dopo deve intervenire rapidamente per ristabilire le condizioni preesistenti.

I benefici del disaster recovery plan sono riconducibili a: migliorare la protezione; minimizzare il tempo di reazione; limitare i danni diretti e indiretti; preservare la salute dei lavoratori; salvaguardare le relazioni strategiche con clienti, fornitori, partner; mantenere una buona reputazione e immagine aziendale; accrescere conoscenza e consapevolezza dei rischi, conseguentemente diminuendo i rischi stessi; migliorare il profilo di rischio interagendo con il mercato finanziario e assicurativo.