18° CONVEGNO
ANNUALE ANRA

ANRA
Associazione Nazionale dei Risk Manager
e Responsabili Assicurazioni Aziendali

FERMA
Federation of European Risk Management Associations

IFRIMA
International Federation of Risk and Insurance Management Associations, Inc.

CAVALCARE LE ONDE DELLA CULTURA GLOBALE ED AZIENDALE

Una strada obbligata per l'Enterprise Risk Manager

Relatore:

Angelo Troiani

Argomento:

L'Attuario nella valutazione del Cyber Risk

Milano, Palazzo Lombardia
19-20 Settembre 2017

Introduzione

Il virus si chiama Petya

Cyber-attacco globale, Eset: Italia il paese più colpito dopo l'Ucraina

BBC Breaking News
@BBCBreaking
Follow

Firms around the globe are reporting a major cyber-attack
bbc.in/2scYQbD
4:55 PM - Jun 27, 2017

SICUREZZA A RISCHIO

Attacco hacker a Unicredit, i criminali potrebbero essere a conoscenza dei debiti dei correntisti

1 Agosto 2017

Cyber-Safe

World reels from massive cyberattack that hit nearly 100 countries

by Jethro Mullen, Selena Larson and Samuel Burke @CNNMoney
May 13, 2017: 3:01 PM ET
Recommend 4.4K

Next cyber-attack could be imminent, warn experts

14 May 2017 | UK
Share

ANSA.it › Tecnologia › Tlc ›
Virus Wannacry: 'Gran Bretagna primo bersaglio dell'infezione' dice l'Europol

Virus Wannacry: 'Gran Bretagna primo bersaglio dell'infezione' dice l'Europol

Microsoft: 'Governi non stocchino pericolosi software'

Cyber risk – Situazione nel mercato

Corporate

- ✓ Cyber risk non è più un rischio emergente
- ✓ Quantificazione del cyber risk volta alla definizione di strategie di risk mitigation
- ✓ Costi elevati legati al miglioramento dei sistemi di sicurezza (a volte comunque insufficiente)

Insurance

- ✓ Primi passi verso la gestione del rischio Cyber
- ✓ Mancanza di dati sulle esposizioni

Le Compagnie sono chiamate ad un'azione immediata per anticipare potenziali rischi futuri.

Affirmative Cyber Risk - Rischio relativo alle polizze che includono esplicitamente la copertura per il cyber risk.

Silent Cyber Risk - Rischio relativo alle polizze già emesse (GL, Property, etc.) che non escludono esplicitamente la copertura per il Cyber Risk.

Prudential Regulation Authority - Findings

Il Cyber Risk è stato oggetto di studio da parte del PRA, tramite il coinvolgimento di una serie di stakeholders (compagnie di assicurazione e riassicurazione, intermediari, consulenti, enti di vigilanza, fornitori di modelli catastrofali e aziende IT che si occupano di cyber security). Tale lavoro si è focalizzato sui rischi di sottoscrizione derivanti dalle polizze che coprono il Cyber Risk (Affirmative e Silent).

Findings

- Il Silent Cyber Risk è un ***rischio materiale***: molte compagnie non hanno a disposizione metodi adeguati per quantificare e gestire tale rischio
- Il business Casualty risulta significativamente esposto al Silent Cyber risk: ciò è dovuto sia allo ***scarso utilizzo delle «esclusioni»*** in sede di stesura delle polizze sia ***all'impossibilità di escludere ragionevolmente perdite*** dovute al Cyber Risk. Alcuni esempi: Directors and Officiers (D&O), Financial Institutions (FI), General Liability (GL) e Professional Indennity (PI)
- Potenziali perdite anche nei settori **Marine, Aviation, Transport e Property.**
- Molte aziende non hanno ancora pianificato ***efficienti strategie di risk appetite*** per la gestione del Cyber Risk (entrambi Affirmative e Silent)
- Le coperture per **l'Affermative Cyber Risk sono ancora poco comprese.**

Modellare scenari per il Cyber risk nel proprio portafoglio

Il processo per lo sviluppo dei possibili scenari è lo stesso per entrambi Affirmative e Silent Cyber Risk: richiede l'identificazione dell'esposizione al rischio e conoscenze nel campo della sicurezza informatica.

1. ***Ipotesi di scenari sistemici plausibili***
2. ***Analisi preliminare degli scenari ipotizzati***
3. ***Selezione dello scenario e costruzione del narrative***
4. ***Logica di calcolo, esposizione e parametri di rischio***

1. Ipotesi di scenari sistemici plausibili

Lista di scenari plausibili da costituire sulla base di:

- Eventi realmente accaduti
- Pubblicazioni accademiche o di industry
- Scenari specifici per l'azienda da definire con gli esperti Cyber

Ogni scenario riporta informazioni riguardo:

- Tipologia di perdita in base al framewrok CAI
- Timeline dell'evento
- Garanzie e LoB impattate

- Gli esperti Cyber forniscono i driver per le perdite (legate a: Costi d'investigazione, IT recovery, costi BI, responsabilità legale, danni fisici, sanzioni, altre spese).

- ✓ **Alcuni scenari sono già disponibili sul mercato**
- ✓ **Scenari specifici per l'azienda**
- ✓ **Verificare la plausibilità degli scenari e garantire che essi siano rilevanti per la stima delle perdite.**

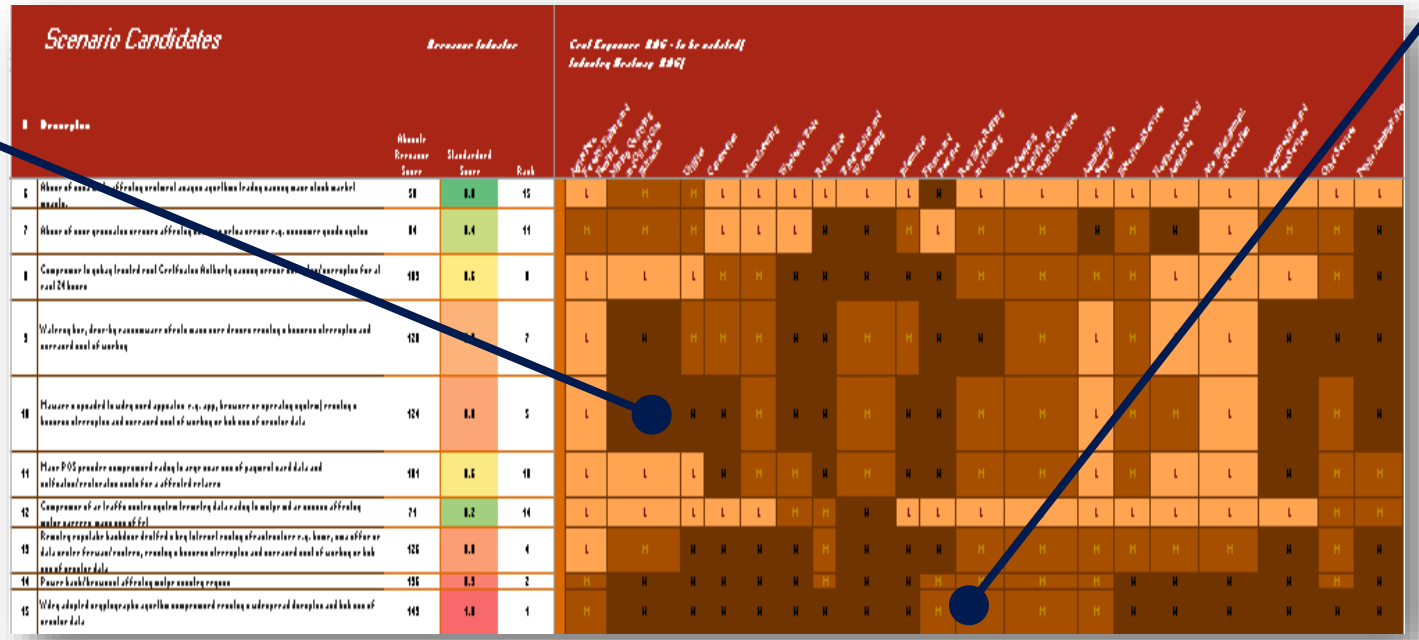
2. Analisi preliminare degli scenari ipotizzati

- ✓ **Analisi preliminare volta all'identificazione degli scenari cui l'azienda è maggiormente esposta**
- ✓ **Driver di scelta possono essere la concentrazione geografica o le industry colpite dall'attacco**

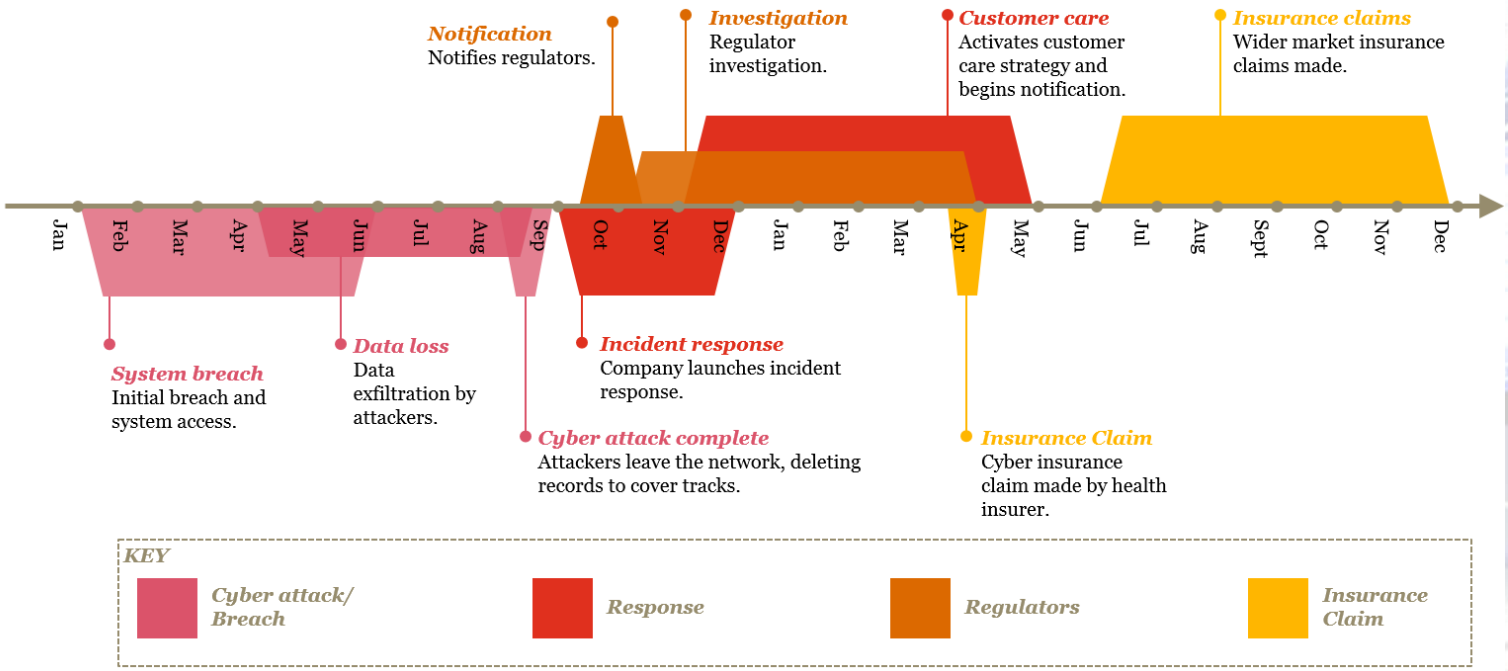
- Focus sulle industry che hanno maggiore dipendenza dalle tecnologie informatiche (Banche, Assicurazioni, Telecomunicazioni, etc.) e sulle aree geografiche maggiormente esposte
- L'analisi degli scenari effettuata con esperti del settore informatico consente una mappatura plausibile dell'impatto sui costi e della perdita dei ricavi

Prioritizzazione delle classi di business impattate dallo scenario per favorire:

- Gli underwriters nella identificazione delle polizze esposte
- I risk manager per definire il modello di valutazione



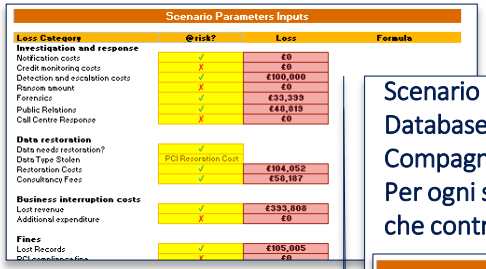
3. Selezione dello scenario e costruzione del narrative



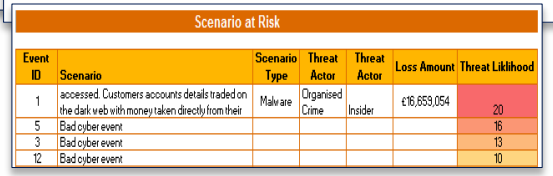
- ✓ Gli scenari considerati più rischiosi vengono selezionati.
- ✓ La produzione di un narrative dettagliato dello Scenario consente di procedere allo sviluppo del un modello di valutazione

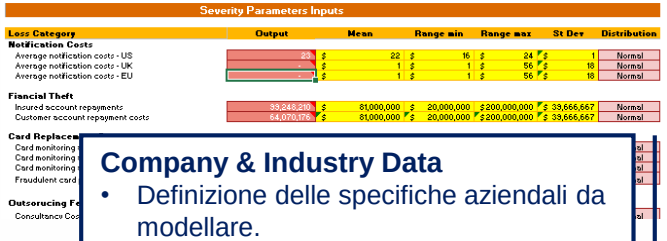
4. Logica di calcolo, esposizione e parametri di rischio

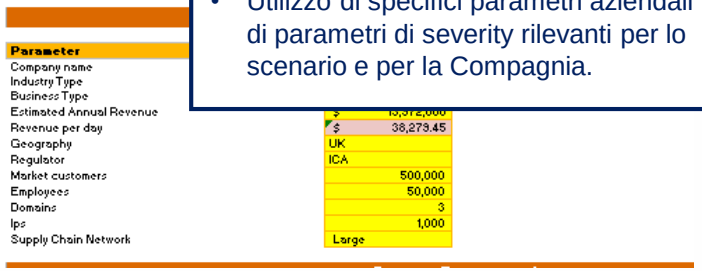
- ✓ **Attraverso l'analisi dei dati e/o il ricorso all'*expert judgement*, derivare i parametri che definiscono la dinamica del modello**
- ✓ **I modelli possono essere deterministici stocastici.**



Scenario Parameters
Database di scenari che possono impattare sulla Compagnia.
Per ogni scenario vengono definite le variabili di calcolo che contribuiscono alla perdita.

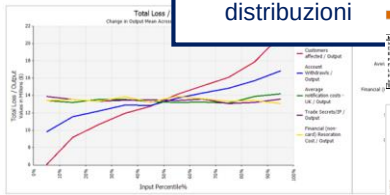


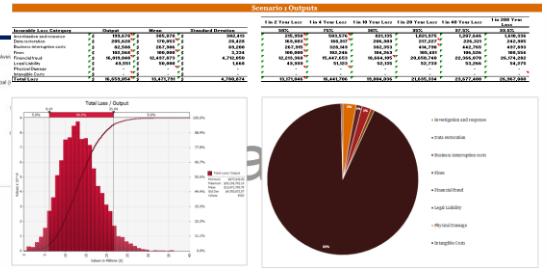




Company & Industry Data
- Definizione delle specifiche aziendali da modellare.
- Utilizzo di specifici parametri aziendali e di parametri di severity rilevanti per lo scenario e per la Compagnia.

Results Module
- Parametri di severity combinati con parametri di calcolo per stimare la perdita relativa a ciascuna categoria.
- La storicità dei dati fornisce informazioni riguardo gli intervalli di confidenza espresso attraverso distribuzioni





Black-out scenario - Narrative example (1 di 3)

Evento

Interruzione della linea elettrica regionale di uno Stato Europeo causata da un malware inserito nei generatori di elettricità. Altri stati europei potrebbero essere indirettamente influenzati a causa della dipendenza energetica dal primo paese.

Plausibilità scenario

Si ritiene che lo scenario sia plausibile in relazione a diversi fattori:

- ✓ **Esistono *situazioni precedenti* di black-out dovute a cyber attack (ad es. il black-out del *sistema elettrico ucraino del 2016*)**
- ✓ **Si tratta di uno scenario ampiamente discusso in letteratura (ad es.*Lloyds e University of Cambridge)*, in quanto ritenuto fondamentale per modellare l'impatto sistemico di un cyber attack. Tale attacco provoca infatti perdite derivanti da un'ampia gamma di sinistri, trasversalmente a diverse linee di busienss.**
- ✓ **Ci sono precedenti di black-out avvenuti in uno stato che hanno avuto *ripercussioni* su altri a causa della *dipendenza energetica* tra i paesi (ad es. il black-out Italiano del 2003 fu causato da un problema tecnico della rete elettrica Svizzera)**

Scenario narrative example (2 di 3)

L'impatto è <u>sistemico</u> in quanto provoca l'estensione del blackout negli altri paesi, attivando una grande quantità di polizze a causa dei numerosi sinistri che ne scaturiscono.

Le potenziali perdite possono essere suddivise in due categorie:
- **Systemic losses**
- **Individual accident losses**

Individual accident losses

- ✓ **Compagnie che producono e distribuiscono energia subiscono danni**
- ✓ **Liability per aziende che hanno fornito i generatori e i software di sicurezza**
- ✓ **Sovraffolamento strutture ospedaliere**

Systemic Losses

- ✓ **Business interruption**
- ✓ **Beni deperibili**
- ✓ **Effetti indiretti su aziende fuori dall'area del blackout**
- ✓ **Household – danni alla proprietà**

Scenario narrative example (3 di 3)

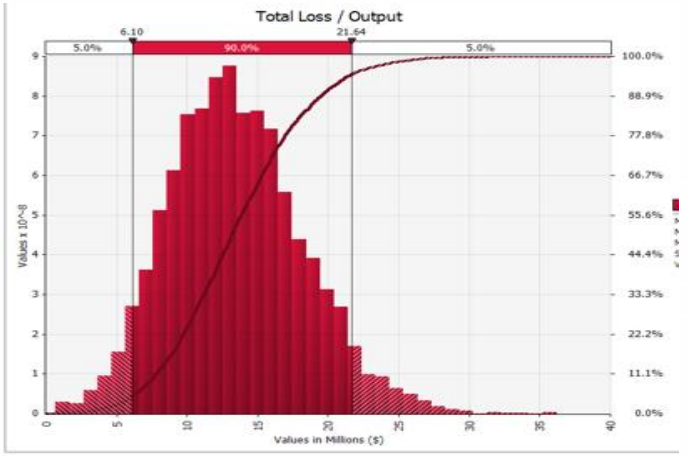
Modello moltiplicativo - Esempio

$$Loss = \sum_i I_i \ * G_i \ * S_i * E_i$$

- ✓ I – ***Industry factor***
- ✓ G – ***Geographical factor***
- ✓ S – ***Size factor (SME or Large corporation)***
- ✓ E – ***Exposure***

Modello simulativo

- ✓ ***Ipotesi probabilistiche sulle distribuzioni dei driver della perdita (ad es. durata del blackout, severity del danno)***
- ✓ ***Definizione dei parametri (Expert judgement)***
- ✓ ***Metodi Monte Carlo di simulazione***
- ✓ ***Ottimizzazione di strategie (ri)assicurative***



Grazie per l'attenzione!

Angelo Troiani