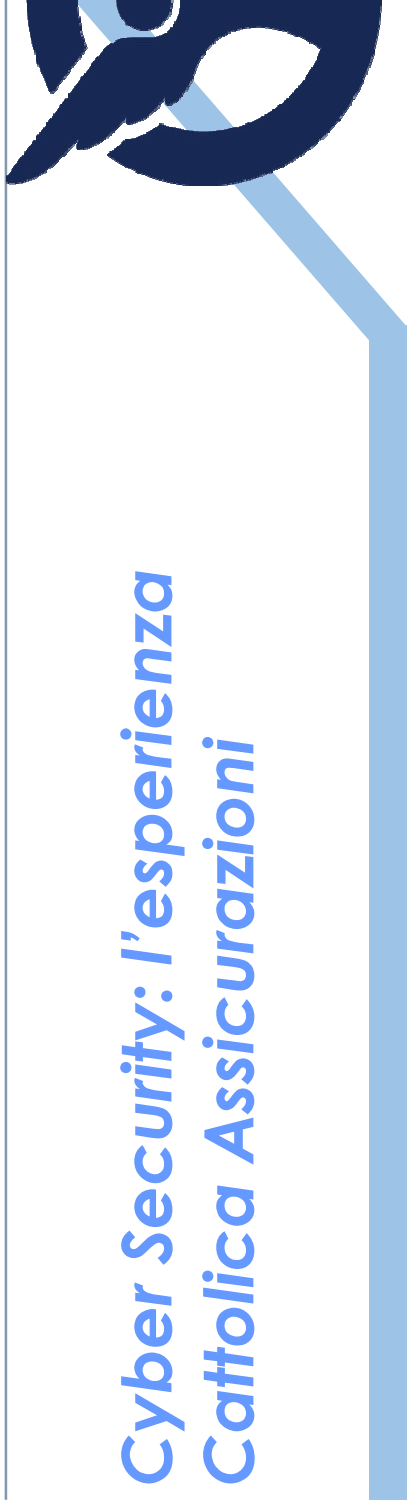


Cyber Security: l'esperienza Cattolica Assicurazioni



Verona, 22 Febbraio 2018



Agenda del documento

- Il Cyber Risk – introduzione, alcuni trend con potenziali impatti sul business (slide 3-4)
- Aspetti normativi e impatti sulle Assicurazioni (slide 5 - 6)
- L'evoluzione dell'approccio al Cyber Risk (slide 7)
- Cyber Risk Management Model (slide 8-14)



Il Cyber Risk è una parte del rischio operativo

Elementi Chiave

Cosa è il Cyber Risk

- Il Cyber Risk appartiene alla classe dei rischi operativi ed è associato alle perdite economiche causate a una organizzazione dalla mancata confidenzialità, disponibilità, integrità di informazioni e/o sistemi informativi, propri o di terzi

Natura del Cyber Risk

- **Accidentale:** l'evento si verifica indipendentemente dalla volontà di tutti i soggetti coinvolti (es. spegnimento server)
- **Deliberata** (es. Cyber Crime): l'evento deriva da azioni volontarie di soggetti allo scopo di raggiungere obiettivi personali di varia natura (es. furto dati sensibili)

Conseguenze

- Il danno economico a un'organizzazione può derivare da malfunzionamenti del proprio sistema IT o essere conseguenza di malfunzionamenti di altri sistemi su cui non si ha controllo
- Principali conseguenze di un evento cyber:
 - Interruzione dell'attività
 - Danno reputazionale/di immagine
 - Perdita quote di mercato
 - Appropriazione identità
 - Azioni legali da terzi
 - Frode (blocco dei sistemi a fini di estorsione)



3

Il Cyber Risk : alcuni trend rilevati nel 2017 che hanno potenziali impatti sul business

Internet of things:

- 200 Billion di dispositivi connessi a Internet entro il 2020
- 90% delle auto saranno connesse a Internet entro 2020
- Primo attacco IoT rilevato nel 2014**
- 90% dei dispositivi connessi colleziona dati personali
- 70% dei dispositivi connessi invia informazioni in chiaro
- 70% dei dispositivi IoT contiene vulnerabilità

Social Media e Social engineering

- 40% degli utenti di social media accetta richieste di amicizie da persone che non conosce
- 78% dei ladri ammette di utilizzare i social media per selezionare le proprie vittime
- 55% di incremento delle campagne di Phishing Campaigns con target i dipendenti delle aziende
- 91% degli attacchi cyber parte da email di phishing
- 85% delle organizzazioni è stata vittima di attacchi phishing
- Il principale veicolo di infezione dei ransomware e altri malware sono gli allegati email
- Una azienda su 3 è stata vittima di CEO fraud emails
- Il 30% dei messaggi di phishing è stato aperto dal destinatario**

Ransomware:

- Il 93% di tutte le mail di phishing contiene ransomware**
- Crescita di attacchi mirati alle Aziende (Ransomware-as-a-service, Targeted Ransomware)
- Il 71% delle Aziende attaccate da ransomware sono state infettate**
- 1 azienda su 5 che hanno pagato il riscatto non hanno recuperato i propri dati
- La richiesta di riscatto medio è salita a 1000+€



4

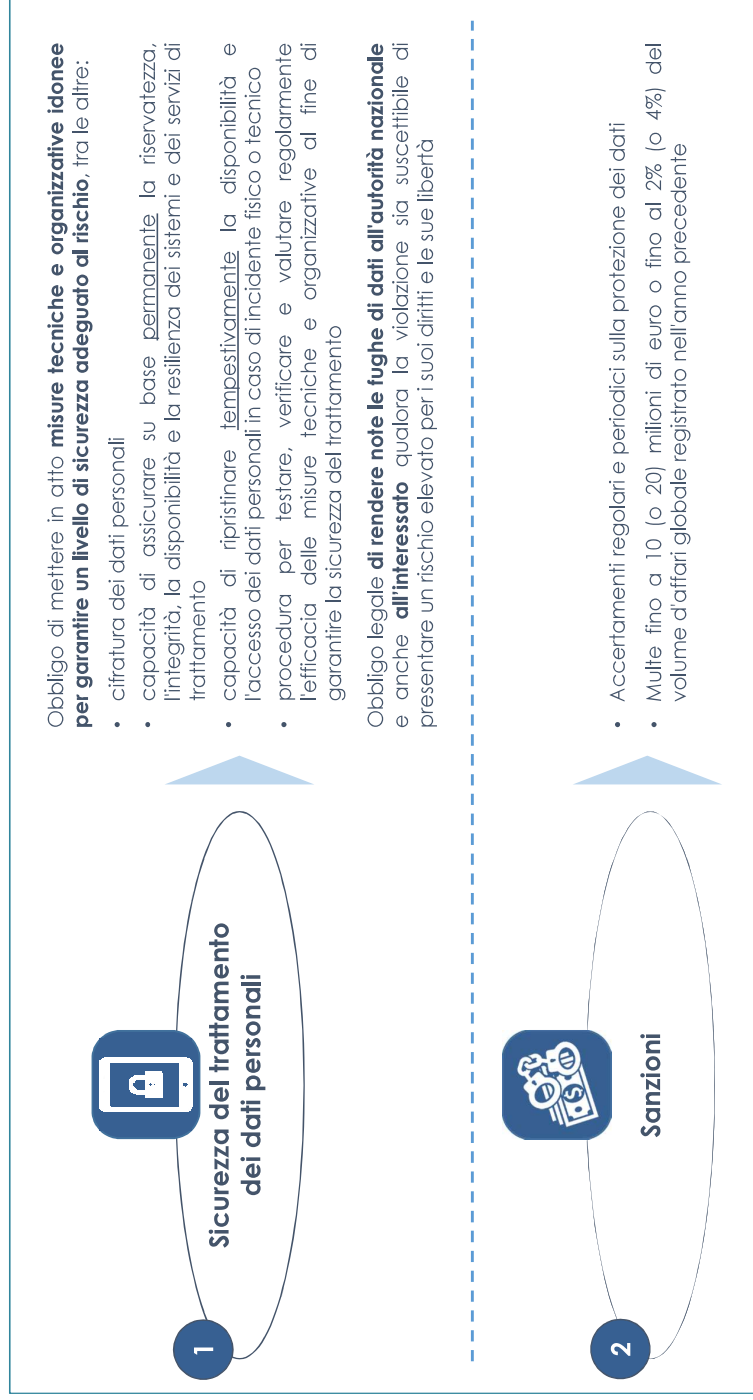
Insider threat:

- La maggior parte degli attacchi più dannosi parte dall'interno delle aziende**
- Le cause principali sono dovute a intenzioni malevole o errori umani. Ad influenzare questo aspetto il dipendente scontento e l'elevato turnover
- Il 93% degli incidenti su cui è stata condotta una indagine (2014/2015) sono stati causati da errori umani

Convergenza della vita lavorativa:

- In incremento la richiesta da parte degli impiegati di utilizzare i dispositivi personali al lavoro (Bring Your Own Device (BYOD), Social Media, Internet of Things)
- Il rischio maggiore con il BYOD risiede nell'impossibilità di controllare i dispositivi personali connessi alle risorse dell'azienda**
- 85% delle imprese permette agli impiegati l'utilizzo dei dispositivi personali al lavoro
- 67% degli impiegati usa il dispositivo personale al lavoro non curandosi delle policy aziendali**
- Dal 2018 il 70% degli utenti svolgerà il proprio lavoro da dispositivi mobili
- 80% dei dispositivi personali non sono gestiti dalle imprese
- La convergenza della vita lavorativa e l'insider threat incrementeranno la percentuale data breach nel futuro

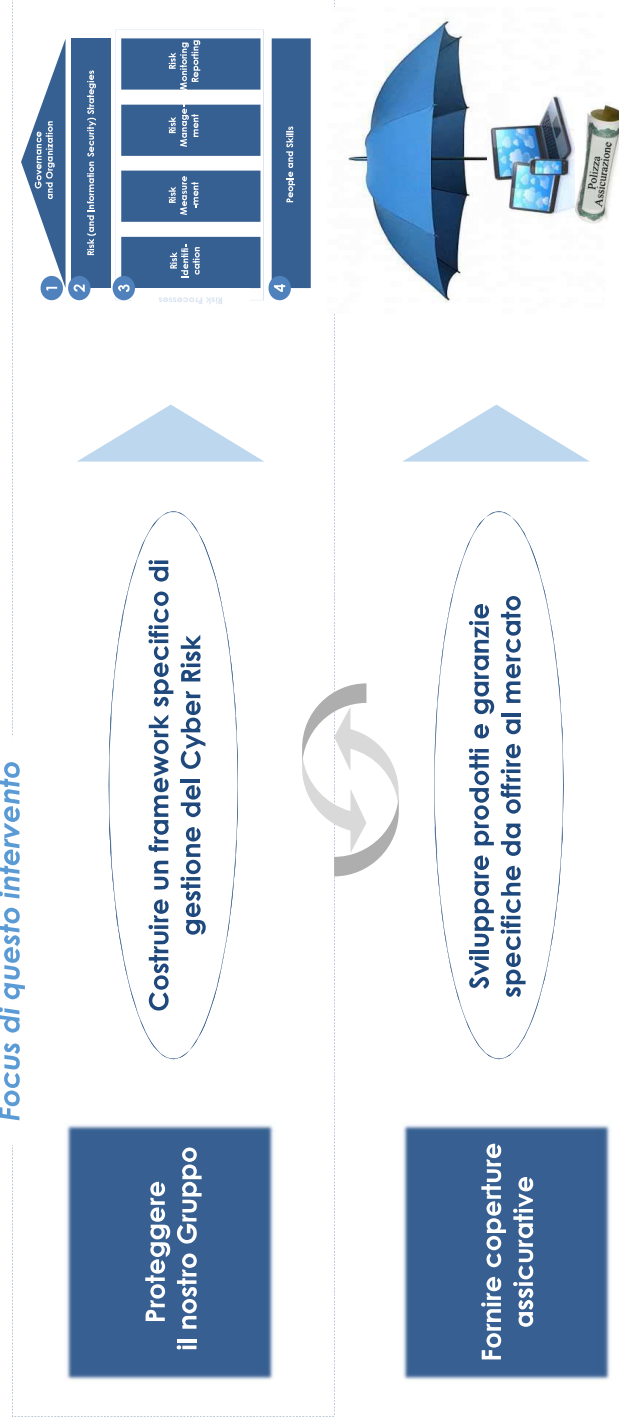
Il Regulator sta imponendo nuovi requisiti alle imprese in tema di protezione dei dati (Regolamento (UE) 2016/679)



5

I due lati del Cyber Risk per le compagnie assicurative: Proteggere se stesse e proteggere gli altri

Focus di questo intervento



Si possono cogliere significative sinergie tra la propria protezione e lo sviluppo di prodotti assicurativi dedicati alle coperture del Cyber Risk



6

Evoluzione approccio Cyber Risk

Approccio alla sicurezza IT «ieri»

Approccio alla sicurezza «IT based»

Oggi: Cyber Security

Approccio alla sicurezza come governo del rischio di cui il rischio IT è parte del contesto

- Focus su sicurezza logica dei dati e sicurezza dell'infrastruttura
- Approccio reattivo al fine di proteggere il patrimonio informativo e non perdere i dati
- Il patrimonio informativo è tutto concentrato nei datacentre e non distribuito
- Mancanza di valutazione e gestione del rischio al di fuori dei sistemi informativi con conseguente difficoltà a spiegare all'alta direzione i potenziali rischi

- Le nuove minacce proattive, l'adozione di dispositivi mobili e nuovi paradigmi tecnologici (es. cloud) impone di valutare e gestire il rischio anche al di fuori dell'area IT
- Il CRO diventa elemento centrale da coinvolgere per la valutazione del rischio
- Rimane il focus su sicurezza logica dei dati e sicurezza dell'infrastruttura
- E' necessario adottare un framework di Mercato che consenta di:
 - ✓ Confrontarsi con il Mercato
 - ✓ Pianificare gli interventi su tutti gli ambiti



7

Il Cyber Risk Management Model è costituito dagli stessi elementi del complessivo modello di gestione dei rischi

1 4 elementi chiave per la gestione del Cyber Risk

1

Governance and Organization

2 Risk (and Information Security) Strategy

Risk Processes

3

Risk Identification

Risk Measurement

Risk Management

Risk Monitoring & Reporting

4

People and Skills

Le linee di difesa necessarie

- Le figure di controllo sono:
 - Audit
 - CRO
 - IT
- Coinvolgimento diretto di CdA e CCR
- E' necessario definire un **Cyber Risk Appetite** con tolleranze e limiti che guidi la Information Security Strategy
- **Richiede un processo specifico di gestione del rischio:**
 - Identificazione delle nuove minacce
 - Misurazione qualitativa e quantitativa dell'esposizione
 - Implementazione sistemi di controllo, azioni di mitigazione e piano di gestione della crisi
 - Monitoraggio costante di KRI specifici

Si richiedono **competenze funzionali e tecniche specializzate**



8

Cyber Risk Management - Governance & Organization



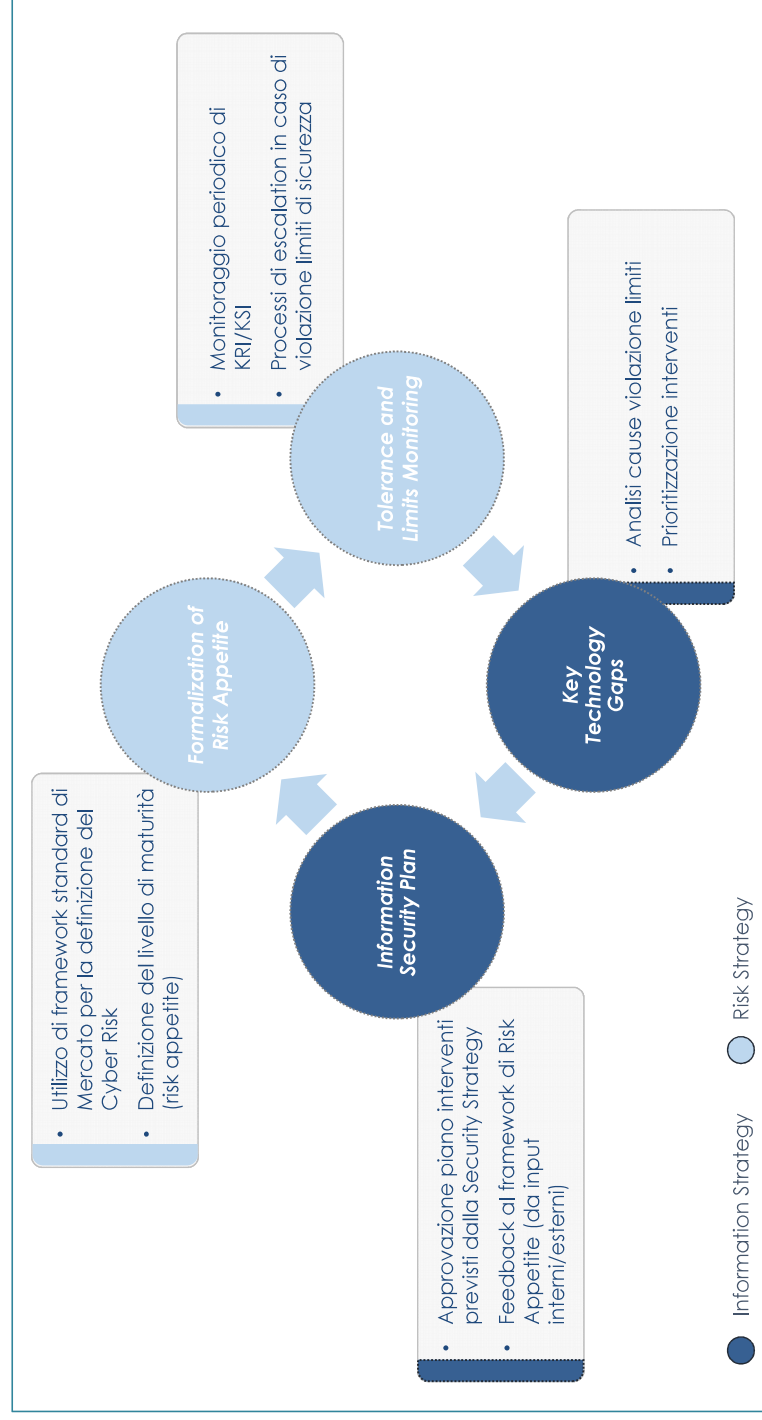
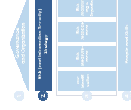
Direzione IT	È la Direzione che eroga per conto delle compagnie assicurative del Gruppo i servizi di information technology
ICT Security	Coordina le attività per l'attuazione delle politiche di sicurezza aziendale e i piani pluriennali di evoluzione della Cyber Security aziendale. Opera il monitoraggio nel continuo degli allarmi
Operational risk management	Effettua la rilevazione e la valutazione dei rischi operativi e monitora le azioni di mitigazioni individuate.
Compliance	Focalizzata sugli aspetti di cambiamento tanto di natura esogena (tipicamente novità di carattere normativo e regolamentare), che di natura endogena, quali, in particolare, progetti di ristrutturazione, apertura di nuovi canali distributivi, introduzione di nuovi applicativi informatici, assicurando da una parte che le novità normative e regolamentari siano recepite tempestivamente ed in maniera efficace, dall'altra che in occasione di cambiamenti interni i rischi di conformità siano sempre tenuti in giusta considerazione e siano mantenuti o migliorati i presidi esistenti.
Funzione privacy di gruppo	- identifica le norme applicabili, i regolamenti, i provvedimenti e le pronunzie delle Autorità in materia di Privacy, con riferimento ai processi e all'operatività del Gruppo; - contribuisce a definire il modello organizzativo complessivo con riferimento alla tutela dei dati personali;



Fonte: Presentazione Ania - workshop su Cyber Risk organizzato da Ivass 21/4/2017

9

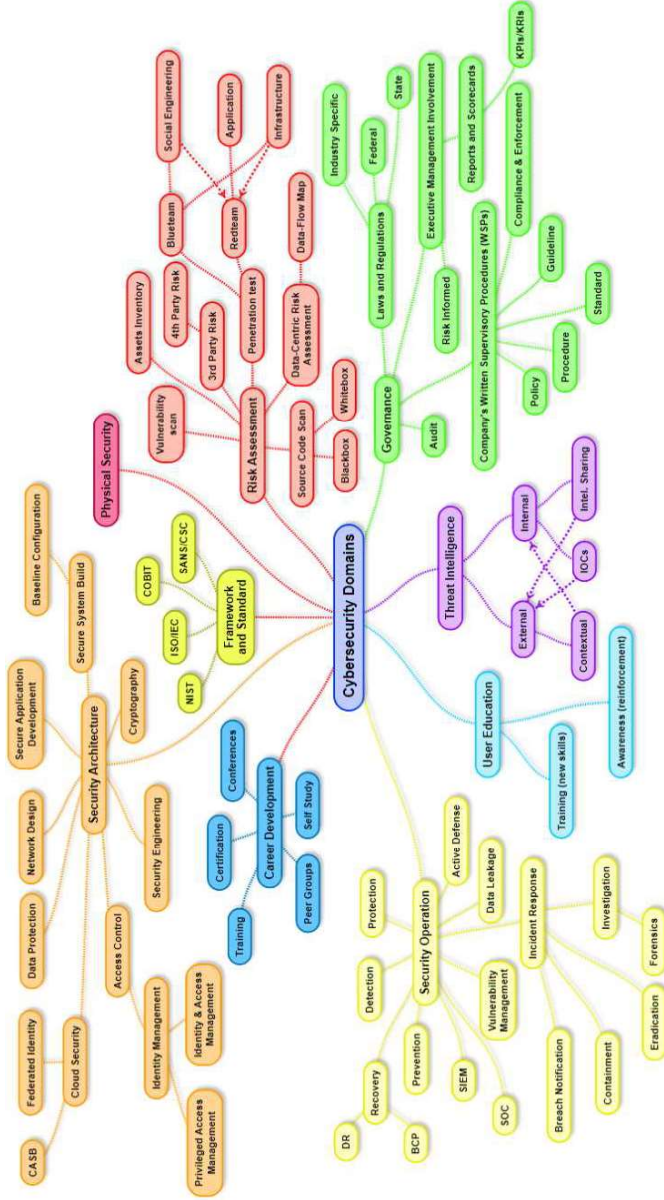
Risk & Information Security Strategy prevede 4 pilastri



10

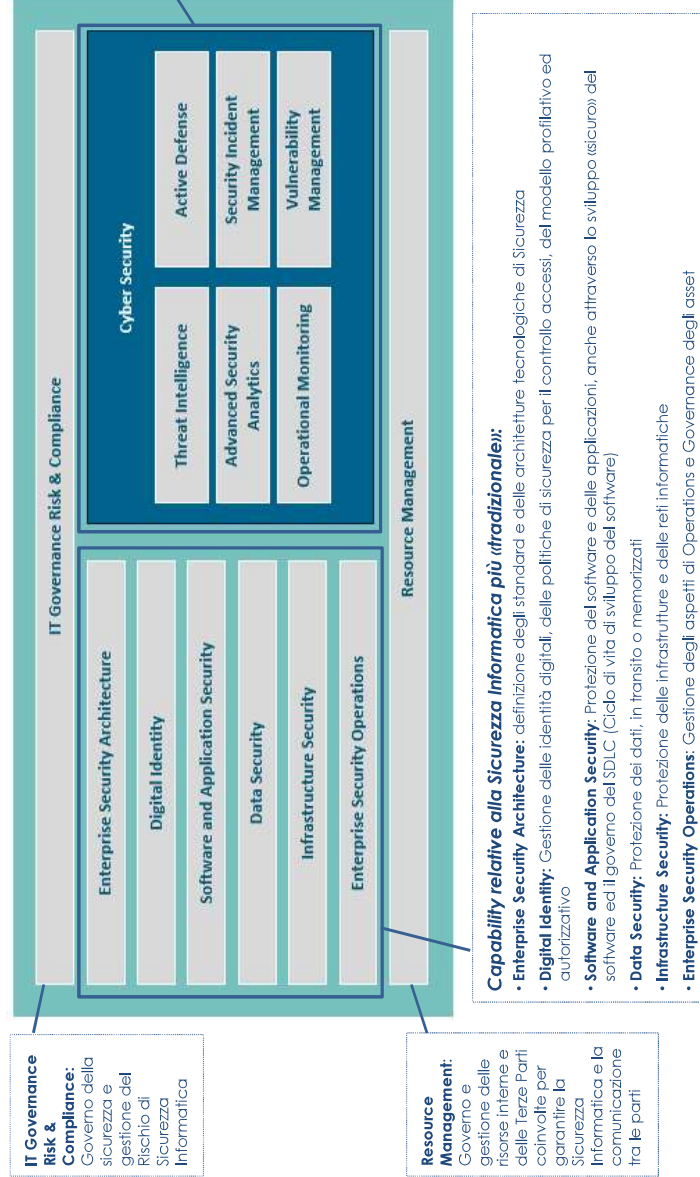
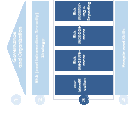
Risk processes: mappa delle interconnessioni degli ambiti della Cyber Security

La vista di alto livello degli ambiti della Cyber Security è rappresentativa ed efficace per spiegare la complessità e le correlazioni logiche di ogni singolo ambito e sotto ambito. Il piano di security strategy di Cattolica e il piano di compliance alla normativa GDPR prevedono numerose iniziative tecnologiche e normative che insistono sulla maggior parte degli ambiti e sotto ambiti rappresentati nella mappa.



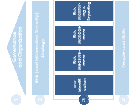
11

Risk processes: implementati e gestiti attraverso l'adozione del modello di riferimento di Mercato NIST



12

Risk Process - Cattolica Security Operation Center



Security Operations Center (SOC) è un centro di competenza da cui vengono forniti servizi finalizzati alla Sicurezza dei Sistemi informativi e garantisce il monitoraggio 24x7 degli eventi e allarmi generati dai sistemi di sicurezza

Minacce e Compliance	In aumento la frequenza degli attacchi cyber, che stanno diventando sempre più sofisticati e dannosi. La normativa è sempre più complessa, vedi introduzione del GDPR e conseguente introduzione di un regime sanzionatorio di non compliance.
Tempo di detection	Copertura 24x7 su 365 giorni. Drastica riduzione del tempo di detection di un incidente di sicurezza. Si stima che, in assenza di un servizio dedicato, il tempo medio di detection di un incident sia superiore ai 250 gg.
Economici	Il servizio in outsourcing fa leva sullo sharing delle risorse su più clienti (si stima che per garantire la medesima copertura, un servizio dedicato gestito internamente richieda un impegno economico pari almeno a 7 volte il servizio in outsourcing). Gli analisti esperti in Cyber Security sono estremamente costosi e scarsamente disponibili nel mercato.
Skill specializzati	Il servizio SOC richiede risorse con forte specializzazione nelle tematiche di sicurezza. Il SOC dispone di analisti di I, II e III livello con adeguate certificazioni. Viene così risolto il problema di shortage di skill disponibili in azienda.

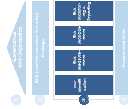
Perché un SOC?

Governance & Compliance	Irrrobustimento della governance della ICT Security con la definizione di processi strutturati di security management facenti leva sui già collaudati strumenti aziendali
Log Management	Log management e analisi 24x7, 365 giorni/anno : analisi selettiva dei log dell'infrastruttura e degli apparati di sicurezza, produzione di report avanzati a scopo di audit, compliance o per attività legali.
Security incident management	Gestione della piattaforma SIEM e continuo tuning e ottimizzazione delle regole di correlazione e degli alert. Predisposizione delle procedure di incident management e supporto nella gestione degli incidenti e nell'indirizzamento delle situazioni di allerta. Servizio di ripristino e forense a fronte di un incidente (CERT : Cyber Emergency Response Team)
Security Operational monitoring	Rilevare le minacce è il primo livello di protezione contro gli attacchi quali, ad esempio, accessi anomali fuori orario di lavoro da parte dei dipendenti, accessi VPN/Workstation, Brute forcing access, accessi anomali da parte degli utenti, sottrazione di dati non autorizzata, accessi fraudolenti, infezioni da malware, botnet
Vulnerability management	Integrazione con i sistemi industriali di governo dell'infrastruttura per indirizzare il ciclo di vita delle vulnerabilità, dalla rilevazione alla mitigazione/risoluzione. Monitoraggio nel continuo delle vulnerabilità infrastrutturali e applicative, valutazione dei rischi, integrazione della valutazione delle vulnerabilità nel ciclo di vita del software e processi di patching nel continuo

Principali innovazioni



Risk Process – SIEM Security Bigdata Analytics



Il Security information and event management (SIEM) è la tecnologia utilizzata per proteggere gli asset e le informazioni dalle minacce avanzate. È il principale strumento utilizzato per le attività di monitoraggio del Security Operation Center (SOC)



- Consolida gli eventi di log e i dati del flusso di rete da migliaia di dispositivi, endpoint e applicazioni distribuiti nella rete. Normalizza e mette in correlazione i dati per identificare le minacce alla sicurezza e utilizza un motore di Analytics avanzato per rilevare anomalie, scoprire minacce avanzate e rimuovere i falsi positivi.
- Integra i servizi di Threat Intelligence che forniscono un elenco degli indirizzi IP potenzialmente sospetti, che includono host malware, botnet, sorgenti spam e altre minacce.
- Consente di correlare le vulnerabilità dei sistemi con i dati di rete, gli eventi dell'infrastruttura, gli eventi applicativi, consentendo di definire le priorità degli incidenti di sicurezza.
- Fornisce visibilità in tempo reale dell'intera infrastruttura IT agevolando il rilevamento delle minacce
- Riduce e definisce le priorità degli alert per focalizzare l'analisi dell'analista di sicurezza su un elenco concreto di incidenti sospetti e con elevata probabilità di manifestazione.
- Consente una gestione delle minacce più efficiente producendo l'accesso ai dati dettagliati e report delle attività degli utenti.

