Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea Triennale in Informatica

Securopoly: un gioco per l'insegnamento della Cybersecurity

Relatore:
Chiar.mo Prof.
Paolo Ciancarini

Presentata da:
Mirko Camporesi

Sessione Unica
Anno Accademico 2015/2016

INDICE

1. INTRODUZIONE

Nel corso di questa tesi verranno presentati vari argomenti legati al mondo della sicurezza informatica e del suo insegnamento. Lo scopo di questo lavoro è presentare la tecnica della gamification e la sua applicazione nel panorama della cybersecurity moderna. Inoltre, verrà proposto un gioco di società chiamato Securopoly che implementa le nozioni descritte e che è basato fortemente sul Framework Nazionale per la cybersecurity, un documento che pone gli standard che ogni organizzazione e ogni azienda dovrebbero soddisfare per essere all'avanguardia nel tentativo di difendersi da attacchi informatici.
In particolare, nel primo capitolo viene effettuata una disamina sulla situazione odierna della cybersecurity per quanto riguarda la sua diffusione e il suo insegnamento. Inoltre, viene definita la gamification come strumento utilizzato per scopi educativi e vengono elencate le caratteristiche fondamentali per una sua corretta applicazione. In seguito, vengono mostrati al lettore alcuni esempi di videogiochi e piattaforme esistenti per l'apprendimento della sicurezza informatica. Alla fine del primo capitolo vengono anche spiegate le ragioni che mi hanno spinto a realizzare Securopoly come strumento per la formazione alla cybersecurity, evidenziando le differenze principali con gli esempi descritti nel paragrafo precedente.
Nel secondo capitolo viene introdotto il Framework Nazionale per la cybersecurity di cui saranno presi in considerazione e presentati tutti quegli aspetti che sono stati fonti d'ispirazione per la realizzazione del gioco di società descritto nel capitolo successivo. In particolare, saranno presentate le principali caratteristiche del Framework Core, ovvero la struttura portante del Framework stesso. Saranno inoltre introdotti temi come i livelli di maturità e le contestualizzazioni del Framework, le cui caratteristiche sono state riprese nello sviluppo del gioco.
Infine nell'ultimo capitolo viene presentato Securopoly, un gioco simil-Monopoly che si propone di essere un valido strumento nell'insegnamento di concetti base di sicurezza informatica sia per ragazzi che vogliono ampliare le loro conoscenze in questo campo, sia soprattutto per persone adulte impiegate in organizzazioni all'interno delle quali la

sicurezza informatica gioca un importante ruolo e non è un fattore da sottovalutare. All'interno di questo capitolo viene quindi descritto lo scopo del gioco e il suo svolgimento, spiegando al lettore tutte le regole previste e le possibili azioni che i giocatori possono compiere durante il loro turno. Verrà poi descritta la preparazione di una partita e fornito un elenco con tutti i materiali necessari. Alla fine del capitolo, sono presenti le condizioni di vittoria e le modalità con cui termina una partita.
È presente inoltre un capitolo dove viene simulata la parte iniziale di una partita tipo, la quale introduce il lettore ai vari eventi che il gioco offre e mostra le principali azioni che i giocatori possono intraprendere durante il corso di una partita.
Per concludere questo documento, sono presenti quattro appendici in cui vengono elencate tutte le carte che il gioco utilizza, mentre una quinta appendice mostra alcuni elementi del Framework Core che sono stati ripresi in Securopoly.

2. APPRENDERE CONCETTI DI SICUREZZA INFORMATICA UTILIZZANDO LA GAMIFICATION

2.1 La diffusione della cybersecurity

Data la sofisticazione e il numero crescente delle minacce informatiche, si fa sempre più attuale la necessità di dare un ruolo attivo anche alle persone non esperte nel campo della sicurezza informatica.
Se poi aggiungiamo che Internet è ormai parte integrante delle nostre vite quotidiane, è evidente che un cittadino non può rimanere all'oscuro di tutti i meccanismi di protezione che servono per utilizzare in maniera adeguata i sistemi e i dispositivi che possiede o con cui ha a che fare. Per questo motivo c'è il bisogno di insegnare sia ai ragazzi giovani che alle persone adulte gli aspetti più importanti del cyberspazio e dei suoi pericoli maggiori.
Se non si crede che ciò sia necessario, basta pensare che le più frequenti vulnerabilità sono dovute a disattenzioni del singolo utente: ad esempio, il 75% delle persone utilizza la stessa password per account diversi, sia a casa che al lavoro; il 7% utilizza una password tra le 100 parole più comuni, il 91% tra le 1000 più comuni e il 99,8% tra le 10000 più comuni [9].
Per tutti questi motivi, al giorno d'oggi, l'utente è l'anello debole all'interno della cybersecurity, dato che in generale viene preferito minimizzare il proprio impegno rendendo le proprie decisioni prevedibili e agendo con ingenuità, senza meditare sul potenziale impatto delle proprie azioni. I cittadini del ventunesimo secolo devono invece incominciare a pensare a loro stessi come "cittadini digitali".
Se ciò è vero per una persona generica, lo è ancora di più per tutti i lavoratori di un'azienda o di un ufficio. I dipendenti sia di piccole che grandi organizzazioni devono essere messi al corrente su una vasta gamma di problemi di sicurezza informatica. Purtroppo però molti utenti solitamente non si interessano delle possibili vulnerabilità presenti su sistemi che utilizzano giornalmente, pensando che dopotutto potrebbero fare molto poco per mitigare questo genere di problemi. Per raggiungere un adeguato livello di consapevolezza della cybersecurity, le organizzazioni devono combattere questa apatia dei loro lavoratori con programmi effettivi

di addestramento.
In generale la consapevolezza sulla sicurezza informatica è generata grazie a una o a una combinazione delle tecniche descritte in seguito:

- **Sessioni teoriche tradizionali**: possono essere lezioni frontali tenute da un istruttore, seminari di approfondimento oppure video-conferenze;
- **Corsi on-line**: rappresentano un approccio centralizzato e omogeneo per tutti. Il loro svantaggio però è quello di diventare una sequenza noiosa di pagine o di slide che non sono adatte a tenere alta l'attenzione dell'utente e in più non permettono interazioni. Per questi motivi, spesso l'utente cerca di completare il ciclo di lezioni in meno tempo e sforzo possibile;
- **Messaggi di sensibilizzazione**: vengono utilizzati nell'ambiente di lavoro per aumentare il livello di consapevolezza riguardo a specifici temi della cybersecurity;
- **Utilizzo di software interattivo**: nella maggior parte dei casi sono videogiochi e si dividono in due categorie:
  - giochi con interazioni in prima persona;
  - simulazioni di gestione delle risorse.

  La maggior parte dei giochi fanno riferimento alla prima categoria, in cui il giocatore affronta una serie di problemi che richiedono di prendere le decisioni corrette per essere superati. Al contrario, i giochi gestionali della seconda categoria chiedono all'utente di amministrare un ambiente virtuale con a disposizione risorse limitate. Se il giocatore agisce in modo giusto migliorando l'ambiente con gli strumenti a disposizione, il gioco lo premia donandogli risorse addizionali.

Mentre un apprendimento tradizionale è basato sui primi tre punti, è solo tramite l'ultima opzione che gli utenti possono davvero mettere le loro abilità alla prova e prepararsi per gli eventi nel mondo reale, senza rischiare di subire danni alle attività e alle risorse coinvolte.
Ad ogni modo, mantenere l'attenzione di una platea sufficientemente a lungo per impartire dei concetti che durino nel tempo è una sfida considerevole, in particolare quando la formazione è obbligatoria e chi sta ascoltando vede l'argomento distante dalle sue competenze. Per tutti questi motivi giochi e videogiochi sono proposti come strumenti coinvolgenti da utilizzare per l'apprendimento [4].

2.2 Cos'è la gamification e come è possibile applicarla in contesti educativi

La gamification è uno strumento per migliorare un servizio specifico mediante l'implementazione di elementi di game design in un contesto dove questi ultimi non sono presenti [9]. Ciò permette di aumentare la interattività con l'utente e rendere l'esperienza più attraente. In aggiunta, quando è progettata e applicata in maniera appropriata, la gamification fornisce la motivazione necessaria per continuare ad utilizzare il servizio a cui è applicata.
Molto importanti, inoltre, sono i contenuti offerti al giocatore. Nel caso della sicurezza informatica, il contesto in cui viene proposto il gioco non deve essere un mondo fittizio ma deve cercare di simulare la realtà. Proprio perchè le tematiche della sicurezza informatica colpiscono la vita di tutti i giorni degli utenti, questi si aspettano giustamente di impegnarsi in compiti realistici e coerenti.
In [7] vengono indicate le caratteristiche e le qualità che un gioco basato sulla gamification dovrebbe avere, di seguito sono riportate quelle più importanti:

- lo scenario del gioco deve essere il più realistico possibile e deve inoltre essere interessante agli occhi del giocatore;
- il gioco deve insegnare i concetti chiavi e sviluppare le abilità del giocatore in modo che quest'ultimo possa imparare dagli errori fatti in passato;
- il gioco deve essere abbastanza complesso per mantenere l'interesse dell'utente ma allo stesso tempo deve anche essere abbastanza semplice da comprendere, per evitare che il giocatore si stanchi e si arrenda;
- gli obiettivi che deve conseguire il giocatore devono essere chiari, anche se il modo per raggiungerli non è completamente esplicito.

Andando più nello specifico, è possibile individuare gli elementi di game design adatti ad un gioco a scopo educativo il cui obiettivo sia quello di trasmettere e insegnare le buone abitudini da prendere nel campo della cybersecurity. Tutte queste caratteristiche sono ampiamente descritte in [1] e [5], e possono essere riassunte nei seguenti punti:

- **Progressione**: individua la motivazione che spinge un giocatore a continuare a giocare e la si può ottenere tramite strumenti come

punti, classifiche generali e distintivi assegnati al termine di particolari missioni;

- **Identificazione**: l'utilizzo di un personaggio/avatar durante il processo di apprendimento può aumentare la partecipazione dell'utente al gioco;
- **Problem-solving**: la capacità di identificare regole generali e pattern è essenziale per lo sviluppo del ragionamento e può tradursi in un più veloce apprendimento di conoscenze pratiche anche al di fuori dell'ambiente in cui si è svolta la formazione;
- **Ambientazione**: un contesto di gioco divertente e avvincente può fare in modo che l'attenzione dell'utente rimanga alta;
- **Narrazione**: una storia che possa creare un legame personale tra l'utente e il suo personaggio.

2.3 Esempi di giochi per l'insegnamento della sicurezza informatica

Andiamo ora a vedere alcuni giochi che mettono in pratica i concetti di cui abbiamo parlato nell'ultima sezione.
Uno degli esempi più importanti è CyberCIEGE [4], un videogioco flessibile e interattivo usato come strumento per aumentare la consapevolezza delle minacce cyber e che può essere affiancato a corsi formativi per la sicurezza informatica.
All'interno del gioco, i giocatori devono amministrare una rete aziendale fittizia in modo tale da permettere ai dipendenti virtuali di svolgere il loro lavoro al meglio delle loro possibilità. In particolare, ai giocatori è richiesto inoltre di difendere la rete da possibili minacce hacker o da virus che possono penetrare all'interno dei sistemi, tutto questo potendo vedere in tempo reale le conseguenze delle loro decisioni. Un esempio di schermata del videogioco è presente in Figura 2.1. In CyberCIEGE sono presenti molteplici scenari preimpostati che possono essere giocati dall'utente e che differiscono tra loro per i diversi eventi ed elementi narrativi che il giocatore può incontrare.
Un altro progetto che intende insegnare come proteggersi dalle minacce del cyberspazio è descritto in [3]. Si tratta di un'implementazione del gioco a quiz televisivo Jeopardy! (da cui é stato derivato il Rischiatutto italiano) che propone la risoluzione di problemi e domande sulla sicurezza

Fig. 2.1: Una schermata di CyberCIEGE

informatica prima di poter accedere al livello successivo. Ha però l'intento di insegnare concetti avanzati che possono essere compresi solo da informatici, non è quindi adatto ad un uso aziendale o per i neofiti.
Un altro esempio su come poter insegnare la cybersecurity ai principianti e a chi non ha modo di partecipare a metodi di insegnamento tradizionali è rappresentato da Code Hunt.
Quest'ultimo viene utilizzato solitamente per aiutare gli studenti a migliorare le loro capacità di programmazione, ma, come riportato in [6], potrebbe essere ampliato per diventare una piattaforma grazie alla quale insegnare concetti di sicurezza informatica. Code Hunt utilizza la gamification, ha una community che supporta attivamente il suo sviluppo e ha un'infrastruttura basata sul cloud che, assieme, forniscono gli strumenti necessari per un apprendimento immediato e senza i costi delle tradizionali infrastrutture. Infatti, è possibile utilizzarlo su una vasta gamma di dispositivi (smartphone, tablet o computer) ed è possibile accedere ai suoi contenuti sempre e ovunque, semplicemente tramite un browser.
Infine, una piattaforma già esistente e supportata dal governo britannico e dal Government Communications HeadQuarters (GCHQ) è CyPhinx [8], un

gioco online per la cybersecurity.

Fig. 2.2: CyPhinx

È stato progettato dalla compagnia no profit Cyber Security Challenge UK, il cui scopo è quello di consentire a più persone di diventare esperti di sicurezza informatica e sviluppare una carriera lavorativa in questo mondo. CyPhinx è letteralmente un grattacielo virtuale con all'interno una serie di sfide che i giocatori devono riuscire a superare per costruire gradualmente il loro curriculum digitale. Queste sfide sono ispirate ad alcuni generi di lavori quotidiani dei professionisti di sicurezza informatica. Un esempio di schermata di CyPhinx è presente in Figura 2.2. Come detto, l'obiettivo di CyPhinx è quello di trovare nuovi giovani talenti e cercare di portarli a considerare un futuro all'interno del settore della cybersecurity.

2.4 Caratteristiche mancanti nei giochi precedenti

Fin'ora abbiamo visto tutte le buone caratteristiche che un gioco necessita per essere qualitativamente appropriato per poter insegnare la cybersecurity. Seppure gli esempi mostrati supportano tali punti, nessuno di questi prende in considerazione altri due elementi che, per quanto mi riguarda, sono fondamentali per l'effettivo successo di un gioco realizzato appositamente per l'educazione dei suoi fruitori.

Il primo di questi due elementi è il fattore "familiarità": con questo termine si intende l'utilizzo all'interno del gioco di strutture largamente conosciute dalla maggior parte dei possibili giocatori, in modo tale che questi ultimi non siano spaesati durante le prime fasi dell'apprendimento. Infatti i videogiochi, per quanto siano strumenti interattivi adatti ad un utilizzo didattico, non possono essere considerati una soluzione efficace per ogni genere di persona che si approccia ad essi, sia per questioni caratteriali del soggetto, sia per il background personale nei confronti di questo media.
L'altro elemento che non è presente negli esempi riportati è il fattore "collettività", ovvero la possibilità di affrontare un percorso condiviso con altre persone per aumentare le proprie conoscenze di sicurezza informatica. In altre parole, i giochi presentati nella sezione precedente, a parte delle classifiche asincrone e confronti basati su statistiche, non prevedono alcuna forma di multiplayer. Questa è una grossa limitazione, in più non viene sfruttata l'occasione di coinvolgere altri utenti con cui condividere i propri sforzi e generare anche una leggera ma significativa spinta competitiva che può innalzare il livello di impegno profuso durante una sessione da parte dei giocatori.
Questi due elementi vengono ottenuti nel gioco da me proposto utilizzando la struttura e le regole basi del Monopoly, gioco di società ampiamente conosciuto e giocabile in gruppo. Prima di presentare le caratteristiche del gioco, è però necessario introdurre il Framework Nazionale per la cybersecurity, che è l'argomento del prossimo capitolo.

3. IL FRAMEWORK NAZIONALE PER LA CYBERSECURITY

È giunto il momento di prendere in considerazione il Framework Nazionale per la cybersecurity, un documento derivato dal "Cybersecurity Framework" del National Institute of Standards and Technology (NIST) americano e prodotto sotto la supervisione di Roberto Baldoni, professore dell'Università "La Sapienza" di Roma.
Durante il corso di questo capitolo saranno discussi solamente gli aspetti che sono stati utilizzati per la realizzazione di Securopoly, pertanto non si può considerare la seguente una descrizione completa del Framework, per la quale si rimanda al documento integrale [2].
Innanzitutto, lo scopo del Framework Nazionale per la cybersecurity è quello di offrire alle organizzazioni un approccio volontario e omogeneo per affrontare la sicurezza informatica al fine di ridurre il rischio legato alla minaccia cyber. È importante comprendere che il Framework non è uno standard di sicurezza, bensì un quadro di riferimento nel quale possono essere inquadrati gli standard e le norme di settore esistenti e future. Pertanto, questo documento ha l'intento di costruire un linguaggio comune per confrontare le pratiche aziendali di prevenzione e contrasto dei rischi cyber. Il Framework può quindi aiutare un'impresa a organizzare un percorso di gestione del rischio cyber, sviluppato nel tempo, in funzione del suo business, della sua dimensione e di altri elementi caratterizzanti e specifici dell'impresa.
I concetti principali all'interno del Framework sono il Framework Core, i livelli di priorità e di maturità e le contestualizzazioni del Framework. Andiamo a vedere in dettaglio uno per uno i concetti appena elencati.

3.1 Framework Core

Il Framework Core rappresenta la struttura del ciclo di vita del processo di gestione della cybersecurity, sia dal punto di vista tecnico sia organizzativo ed è strutturato gerarchicamente in Function, Category e Subcategory (le prime due sono schematizzate nella Figura 3.1). Le Function, concorrenti e

continue, sono: Identificare, Proteggere, Rilevare, Rispondere e Recuperare. Esse costituiscono le principali tematiche da affrontare per operare un'adeguata gestione del rischio cyber in modo strategico. Il Framework quindi definisce, per ogni Function, Category e Subcategory, processi e tecnologie da mettere in campo per gestire la singola Function.

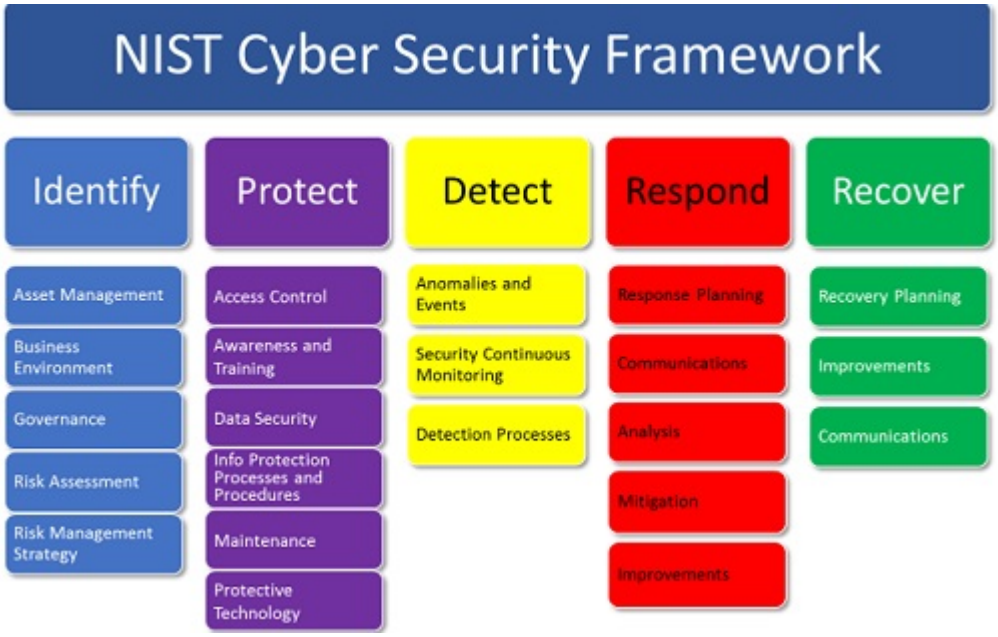

Fig. 3.1: Function e relative Category del Framework Core

Di seguito è riportata una breve descrizione delle 5 Function:

- **Identificare**: La Function Identificare è legata alla comprensione del contesto aziendale, degli asset che supportano i processi critici di business e dei relativi rischi associati. Tale comprensione permette infatti a un'organizzazione di definire risorse e investimenti in linea con la strategia di gestione del rischio e con gli obiettivi aziendali. Le Category all'interno di questa Function sono:
  - Censimento delle Risorse;
  - Definizione degli Obiettivi;
  - Definizione della Politica Aziendale per la Cybersecurity;
  - Valutazione del Rischio;
  - Strategia per la Gestione del Rischio.

- **Proteggere**: La Function Proteggere è associata all'implementazione di quelle misure volte alla protezione dei processi di business e degli asset aziendali, indipendentemente dalla loro natura informatica. Le Category all'interno di questa Function sono:
  - Controllo degli Accessi;
  - Formazione e Addestramento del Personale;
  - Sicurezza dei Dati;
  - Attivazione e Aggiornamento delle Politiche di Sicurezza;
  - Manutenzione dei Sistemi Informativi;
  - Tecnologie Aziendali per la Protezione.
- **Rilevare**: La Function Rilevare è associata alla definizione e attuazione di attività appropriate per identificare tempestivamente incidenti di sicurezza informatica. Le Category all'interno di questa Function sono:
  - Rilevamento delle Anomalie;
  - Monitoraggio Periodico dei Sistemi Informativi;
  - Consistenza dei Processi di Rilevamento.
- **Rispondere**: La Function Rispondere è legata alla definizione e attuazione delle opportune attività per intervenire quando un incidente di sicurezza informatica viene rilevato. L'obiettivo è contenere l'impatto determinato da un potenziale incidente di sicurezza informatica. Le Category all'interno di questa Function sono:
  - Piano di Risposta a un Incidente;
  - Coordinamento delle Operazioni di Risposta;
  - Analisi degli Incidenti;
  - Contenimento e Mitigazione di un Incidente;
  - Miglioramenti al Piano di Risposta.
- **Recuperare**: La Function Recuperare è associata alla definizione e attuazione delle attività per la gestione dei piani e per il ripristino dei processi e dei servizi impattati da un incidente. L'obiettivo è garantire la resilienza dei sistemi e delle infrastrutture e, in caso di incidente, supportare il recupero tempestivo delle operazioni legate al business. Le Category all'interno di questa Function sono:

- Piano di Ripristino;
- Miglioramenti al Piano di Ripristino;
- Gestione delle Comunicazioni in seguito a un Incidente.

Sempre all'interno del Framework Core troviamo i profili, che rappresentano il risultato della selezione, da parte di un'organizzazione, di specifiche Subcategory del Framework. I profili possono essere utilizzati come opportunità per migliorare lo stato di sicurezza mettendo a confronto un profilo attuale (anche detto corrente), con un profilo desiderato (anche detto target). Per sviluppare un profilo, un'organizzazione deve esaminare ciascuna delle Subcategory e, sulla base del proprio business e della valutazione dei propri rischi, determinare quali sono da implementare e quali non sono applicabili nel proprio contesto. Il profilo attuale può quindi essere utilizzato per definire priorità e misurare i progressi verso il profilo desiderato.

3.2 I livelli di Priorità e di Maturità

I livelli di priorità definiscono qual è l'importanza specifica con cui si deve affrontare ogni singola Subcategory del Framework Core. Inoltre, questi livelli permettono di supportare le organizzazioni e le aziende nell'identificazione preliminare delle Subcategory da implementare per ridurre maggiormente i livelli di rischio a cui sono sottoposte, bilanciandone l'impegno da profondere per la loro attuazione.
Non essendo però stati utilizzati nella creazione di Securopoly, dato che sono sì un fattore importante per le aziende ma non per l'addestramento dei dipendenti alla cybersecurity, non verranno approfonditi ulteriormente.
I livelli di maturità, invece, permettono di fornire una misura della maturità di un processo di sicurezza, di attuazione di una tecnologia specifica o una misura della quantità di risorse adeguate impiegate per l'implementazione di una data Subcategory. I livelli di maturità forniscono un punto di riferimento in base al quale ogni organizzazione può valutare la propria implementazione delle Subcategory e fissare obiettivi e priorità per il loro miglioramento.
Le diverse modalità con cui si può implementare ogni singola Subcategory del Framework Core sono infatti identificate da uno specifico livello di maturità. Tipicamente livelli di maturità maggiori richiedono uno sforzo maggiore, sia dal punto di vista economico che di gestione.

3.3 Le contestualizzazioni del Framework

Creare una contestualizzazione del Framework (per un settore produttivo, per tipologie di azienda o per una azienda singola), significa selezionare le Function, Category e Subcategory del Framework Core pertinenti, specificando i livelli di priorità e di maturità adatti al contesto di applicazione.
Elenchiamo quindi le operazioni necessarie per l'applicazione corretta del Framework da parte di una azienda:

1) Identificare una contestualizzazione del Framework adatta per l'azienda, elencando tutte le Function/Category/Subcategory che sono pertinenti per l'organizzazione e definendo i livelli di priorità e di maturità per l'implementazione delle Subcategory selezionate;

2) Determinare il profilo corrente basato sulla contestualizzazione del Framework adottato e analizzare il rischio associato;

3) Individuare il profilo target e determinare il gap rispetto al profilo corrente.

4. SECUROPOLY: UN GIOCO SIMIL-MONOPOLY BASATO SUL FRAMEWORK NAZIONALE

Avendo introdotto il Framework Core e tutte le sue caratteristiche relative, vediamo ora come queste vengano applicate al funzionamento di Securopoly. All'interno di questo capitolo verranno quindi racchiuse tutte le regole e verrà spiegato esaustivamente lo svolgimento del gioco e i suoi obiettivi. Inoltre, verranno elencati i componenti necessari, verrà spiegato come preparare una partita di Securopoly e saranno presenti anche esempi di alcune situazioni particolari di gioco che avvengono nel corso di una partita.

4.1 Scopo del gioco

Come già detto in precedenza, l'obiettivo di Securopoly è quello di sensibilizzare i giocatori verso temi di sicurezza informatica solitamente trascurati.
Chiunque sia interessato ad approfondire certi argomenti può utilizzare questo gioco per apprendere quali sono le linee guida suggerite dal Framework Nazionale per la cybersecurity per le piccole e medie imprese. Proprio per il fatto che Securopoly è basato su questo specifico documento, il gioco è particolarmente indirizzato a manager o responsabili del settore informatico di un'organizzazione che hanno poteri decisionali e sono interessati alla messa in sicurezza dell'impresa di cui fanno parte. Il gioco cerca di mettere di fronte queste figure a situazioni verso le quali solitamente non si presta abbastanza attenzione e che possono portare delle vulnerabilità nei sistemi informatici.
Proprio per dare un maggiore senso di immedesimazione, i giocatori vestono i panni di un manager di un'organizzazione fittizia a cui viene richiesto di migliorare la sicurezza dell'azienda di cui fanno parte. Partendo quindi da una situazione iniziale diversa per ogni giocatore, ognuno di questi dovrà aumentare le difese della propria impresa fino a raggiungere l'obiettivo prefissato.
Per fare ciò, è necessario aumentare il livello delle varie caselle presenti sul tabellone di gioco contraddistinte da 5 colori diversi che rappresentano

esattamente le 5 Function del Framework Core viste nel capitolo precedente. In particolare, ogni casella appartenente a uno di questi colori rappresenta una Category del Framework Core. Essendo invece le Subcategory troppo numerose, è stato necessario compiere una semplificazione rispetto al Framework: i livelli di maturità sono stati quindi attribuiti alle Category, cercando comunque di far risaltare le Subcategory con priorità maggiore all'interno dei livelli così definiti.
I colori che identificano le Function nel Framework Core sono ripresi tali e quali anche in Securopoly:

- Il Blu identifica la Function "Identificare";
- Il Viola identifica la Function "Proteggere";
- Il Giallo identifica la Function "Rilevare";
- Il Rosso identifica la Function "Rispondere";
- Il Verde identifica la Function "Recuperare";

È importante fin da subito far notare una delle differenze più marcate che ha Securopoly rispetto al Monopoly originale: ogni singola casella del tabellone di gioco viene condivisa da ogni giocatore, non è quindi possibile "possedere" una particolare casella perchè questa individua la stessa Category nelle diverse aziende dei giocatori. Infatti, come vedremo nel dettaglio in seguito, ogni giocatore potrà aumentare il livello di una particolare casella in maniera indipendente e parallela agli altri giocatori.

4.2 Componenti

In questa sezione sono elencati brevemente i materiali e le varie componenti che formano Securopoly per dare al lettore un'anticipazione del contenuto che verrà utilizzato durante il corso di una partita.
Il gioco è quindi formato da:

- **Tabellone di gioco**: è in gran parte fedele a quello del Monopoly classico, ma in questo caso, come è stato già accennato in precedenza, è composto da caselle che rappresentano le Category del Framework Core suddivise nelle rispettive 5 Function a cui è stato assegnato un colore diverso per ognuna. In aggiunta a queste, sono presenti le classiche caselle "Imprevisto" e "Probabilità", con l'aggiunta delle caselle "Mercato". Per ognuna di queste categorie è prevista una zona dove posizionare le carte del rispettivo mazzo. In aggiunta, è presente

uno spazio per le carte "Mercato" attive. Infine, sono previste tre caselle bonus in tre angoli differenti del tabellone e due caselle "Doppio Tiro" che saranno spiegate in seguito. Un'immagine integrale dell'intera plancia è visibile in Figura 4.1;

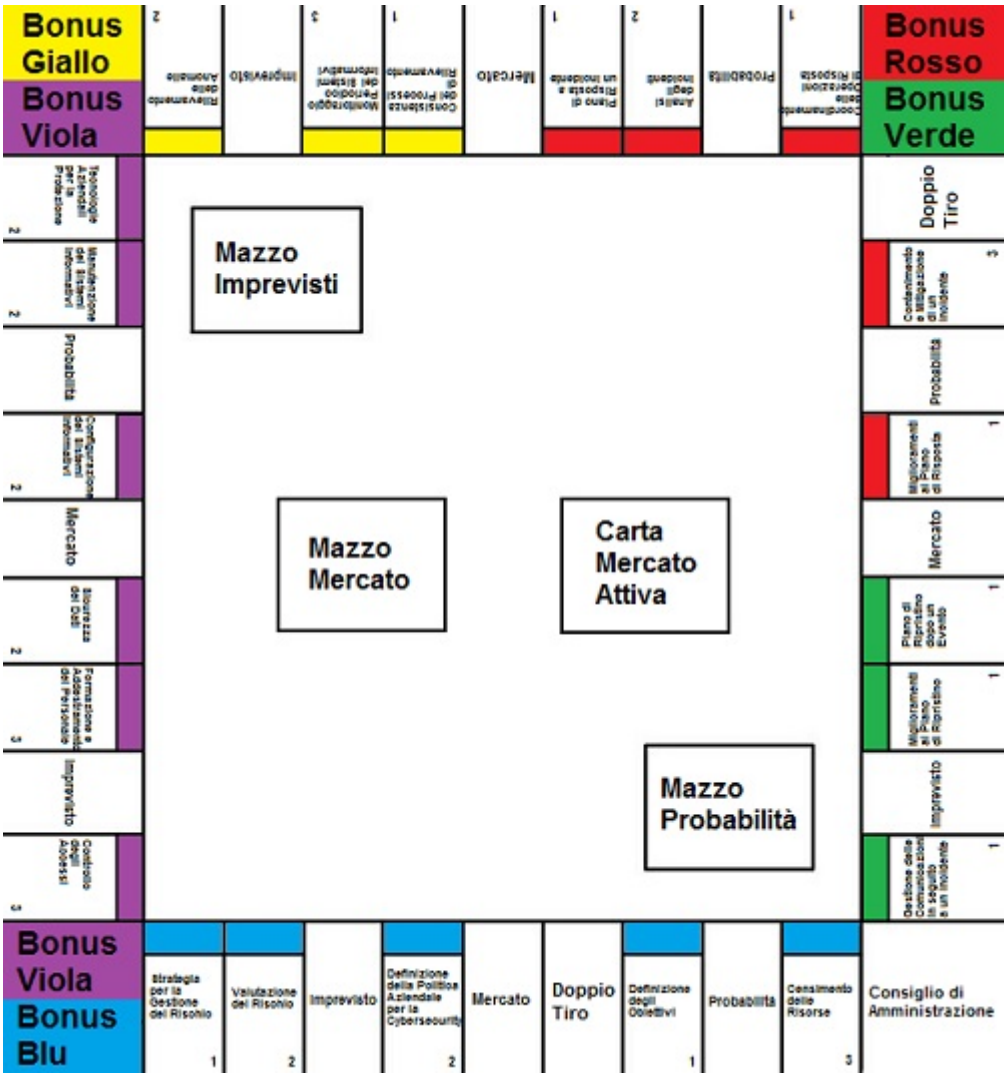

Fig. 4.1: Tabellone di Gioco

- **Pedine dei giocatori**;
- **Marcatori**: di colore diverso per ogni giocatore, vengono utilizzati per indicare il livello di maturità di ogni singola Category. Infatti, su ogni marcatore viene raffigurato un numero da 1 a 3 che indica

proprio il livello di maturità rappresentato. Esempi di marcatori sono visibili in Figura 4.2

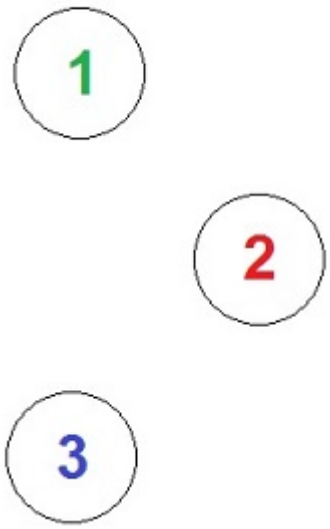

Fig. 4.2: Marcatori appartenenti a giocatori diversi

- **Segnalini "Rischio"**: indicano le vulnerabilità che possono accumularsi all'interno dell'azienda;
- **Segnalini "Doppio tiro"**: possono essere utilizzati per tirare due volte il dado;
- **12 carte "Imprevisto" in doppia copia (24 carte totali)**: una descrizione completa di tutte le carte "Imprevisto" è presente nell'Appendice A;
- **12 carte "Probabilità" in doppia copia (24 carte totali)**: una descrizione completa di tutte le carte "Probabilità" è presente nell'Appendice B;
- **10 carte "Mercato"**: una descrizione completa di tutte le carte "Mercato" è presente nell'Appendice C;
- **10 carte "Profilo Attuale" e 10 carte "Profilo Target"**: le prime individuano la situazione iniziale dell'azienda, le seconde sono gli obiettivi che i giocatori devono raggiungere. Una descrizione

completa di tutte le carte "Profilo Attuale" e "Profilo Target " è presente nell'Appendice D;

- **1 dado a sei facce**.

4.3 Preparazione

In questo paragrafo vengono descritte le azioni iniziali per preparare una partita e viene spiegato in che modo disporre i vari componenti del gioco che abbiamo appena visto.
Innanzitutto, ogni giocatore sceglie un colore e prende i marcatori e la pedina a esso relativi. Questi colori non hanno nessuna relazione con i cinque presenti sul tabellone e che invece indicano le Function del Framework Core, ma servono semplicemente a distinguere i giocatori tra loro.
Fatto ciò, vengono posizionate le pedine nella casella "Consiglio di Amministrazione" che è la casella di partenza (infatti corrisponde al "Via!" del Monopoly classico).
A questo punto, i mazzi delle carte "Profilo Attuale" e "Profilo Target" vengono mischiati separatamente e viene distribuita una carta da entrambi i mazzi a ogni giocatore. Come è chiaro dal nome, queste carte rappresentano esattamente i profili attuali e target come descritti all'interno del Framework Core durante il secondo capitolo. Infatti il primo mazzo andrà a individuare la situazione iniziale dell'azienda e mostrerà al giocatore quali Category sono state già implementate e con quale livello di maturità. Il secondo mazzo, invece, mostra quali sono gli obiettivi futuri dell'organizzazione e sarà compito del giocatore cercare di raggiungerli. In particolare, per ognuna delle cinque Function è indicato il punteggio richiesto che il giocatore deve raggiungere. Questo punteggio è calcolato sommando tutti i livelli di maturità delle Category appartenenti alla Function relativa. Un esempio di carta "Profilo Target" è mostrata in Figura 4.3.
Facciamo un esempio e prendiamo in considerazione la Function "Rilevare" e le sue tre Category. Sul "Profilo Target" di un giocatore è indicato che tale Function deve avere un punteggio pari o superiore a 4. Fin'ora il giocatore è riuscito a posizionare un marcatore di livello 2 sulla Category "Monitoraggio dei Sistemi Informativi" e un marcatore di livello 1 sulla Category "Rilevamento delle Anomalie". Per raggiungere l'obiettivo indicato sulla sua carta "Profilo Target", il giocatore dovrà aumentare ancora di un livello di maturità una qualsiasi delle tre Category appartenenti alla Function "Rilevare".

Fig. 4.3: Un esempio di carta Profilo Target, che indica per ogni Function il punteggio che il giocatore deve raggiungere per vincere la partita

Dopo aver ricevuto queste due carte, ogni giocatore conserva segretamente il proprio "Profilo Target" mentre rivela davanti a sè il "Profilo Attuale" con cui andrà a posizionare i propri marcatori nelle caselle indicate. Un esempio di quest'ultima tipologia di carta è visibile in Figura 4.4.
In seguito, tutte le carte "Profilo Attuale" e le carte "Profilo Target" non utilizzate vengono messe da parte. Si dividono ora le altre carte presenti nei rispettivi mazzi, ovvero "Probabilità", "Imprevisti" e "Mercato". Tutti i mazzi vengono mescolati e riposti nelle rispettive zone del tabellone.
A tutti i giocatori vengono consegnati come quota simbolica 200 euro che saranno i fondi iniziali assegnati dall'azienda per lo sviluppo della sicurezza.
Infine, ogni giocatore tira un dado per stabilire chi sarà il primo a giocare. Chi ottiene il numero più alto sarà il primo a partire, in seguito il gioco prosegue in senso orario.

4.4 Svolgimento

Questa sezione è probabilmente la più importante dell'intero capitolo, dato che verrà spiegato come si svolge un turno generico di un giocatore e gli effetti di ogni tipologia di casella su cui si può capitare. All'inizio del proprio turno, la prima azione svolta dal giocatore è quella di lanciare il dado a sei facce e muoversi in senso orario sul tabellone per il numero di caselle ottenuto. A seconda della casella su cui si capita, il giocatore dovrà compiere azioni diverse:

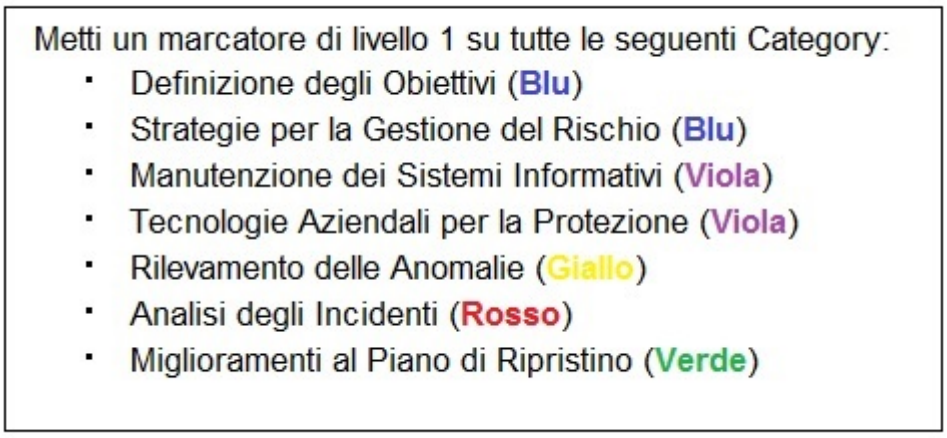

Fig. 4.4: Un esempio di carta Profilo Attuale, dove vengono indicate tutte le Category già in parte sviluppate con cui il giocatore incomincerà la partita

- **Casella Category**: se la pedina termina su una casella che individua una delle Category del Framework Core, come per esempio la casella mostrata in Figura 4.5, il giocatore può scegliere se aumentare di uno il livello di maturità di tale caratteristica pagando una certa somma oppure può decidere di non investire in quel particolare campo della sua azienda (magari perchè non rientra nel suo "Profilo Target", o perchè vuole dare precedenza ad altre Function, o ancora perchè vuole semplicemente conservare le proprie risorse economiche per il futuro). I costi necessari per aumentare il livello di maturità di una particolare Category sono i seguenti:

  - Per portare la casella al livello di maturità 1 è necessario spendere 20 euro.
  - Per portare la casella al livello di maturità 2 è necessario spendere 40 euro.
  - Per portare la casella al livello di maturità 3 è necessario spendere 60 euro.

  Come è possibile notare, maggiore è il livello di maturità che si vuole ottenere, maggiore è anche lo sforzo economico che bisogna sostenere. Se il giocatore decide di investire nella Category su cui è capitato, mette uno dei propri marcatori corrispondente al livello di maturità pagato all'interno della casella in cui si trova.

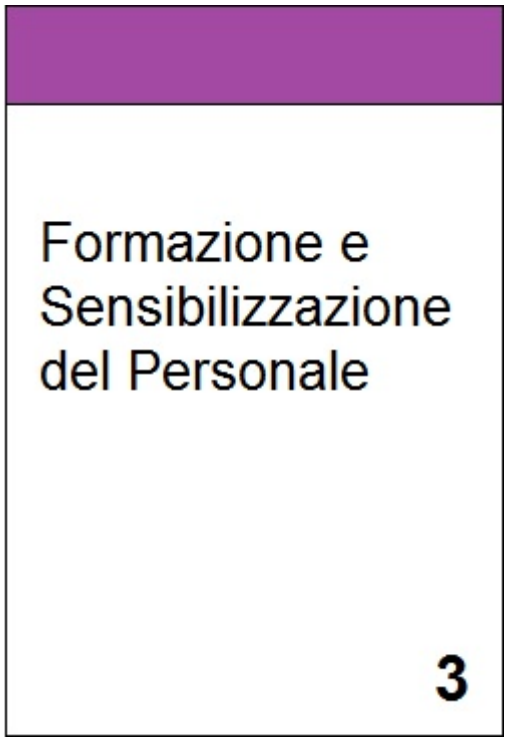

Fig. 4.5: Una delle Category che compongono il tabellone: il Viola denota la Function "Proteggere", il numero 3 denota il livello di maturità massimo, il titolo della casella è un riferimento diretto alla Category del Framework Core

Non tutte le Category possono essere "potenziate" fino al livello 3, ma, come indicato sul Framework Nazionale, possono essere limitate al livello 1 o 2. È possibile vedere quale è il livello massimo previsto da ogni Category grazie al numero presente in basso a destra su ogni casella di questa tipologia. Inoltre, ai lati del tabellone è presente una guida che sintetizza brevemente per ogni Category quali vantaggi attribuisce all'azienda a seconda del suo livello di maturità. Questo permette al giocatore di avere una conoscenza maggiore e apprendere quali sono gli effetti pratici nel migliorare il livello di maturità di una particolare Category. La descrizione di ogni livello di maturità delle Category presenti sul tabellone è elencata nell'Appendice E.
Nel caso in cui un giocatore capitasse su una Category che ha già precedentemente portato al suo livello massimo, gli viene consegnato direttamente un bonus, dato che la sua azienda è in grado di padroneggiare tale caratteristica e questo ha effetti positivi sulla efficienza delle operazioni. Il bonus dipende da quanto è il livello

massimo della casella: se il livello di maturità massimo della Category è 1, il bonus equivale a 10 euro; se il livello di maturità massimo della Category è 2, il bonus equivale a 20 euro; altrimenti, se il livello di maturità massimo della Category è 3, il bonus equivale a 30 euro. Oltre al bonus, il giocatore può decidere di investire in un'altra Category che condivide lo stesso colore della casella su cui è attualmente, pagando il rispettivo costo.

- **Casella Probabilità/Imprevisto**: se la pedina termina su una casella "Imprevisto" oppure "Probabilità", il giocatore deve pescare la prima carta del relativo mazzo e seguire le istruzioni riportate in essa. Per esempio, supponiamo che la pedina del giocatore finisca su una casella "Imprevisto". Il giocatore pesca dal relativo mazzo la carta mostrata in Figura 4.6: nella parte superiore è presente una breve descrizione dell'evento che spiega al giocatore in quale contesto si trova; nella parte inferiore sono riportati gli effetti che la carta ha sul gioco stesso e vengono indicate le azioni che il giocatore deve seguire. In questo caso specifico, al giocatore è richiesto di possedere la Category "Formazione e Addestramento del Personale" almeno al livello di maturità 1. Se la richiesta è soddisfatta, il giocatore non incorre in nessuna penalità, altrimenti gli viene assegnato un segnalino "Rischio" (vedremo più avanti che effetti hanno questo genere di segnalini).

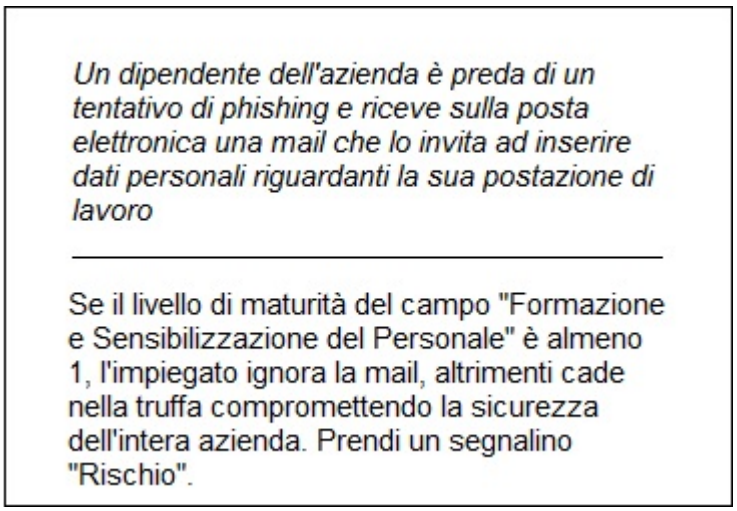

Fig. 4.6: Un esempio di carta Imprevisto

Una grossa parte dell'apprendimento è quindi affidata alle carte "Imprevisto" e "Probabilità" che, attraverso la narrazione di possibili

eventi, mettono in guardia il giocatore su quali sono i principali pericoli che possono avvenire in qualsiasi momento durante l'attività dell'azienda e quali sono le buone abitudini da seguire per evitare che si verifichino incidenti di natura informatica.

- **Casella Mercato**: se la pedina termina su una casella "Mercato", il giocatore deve pescare la prima carta del relativo mazzo e posizionarla a faccia in su nella rispettiva zona. Questa tipologia di carte hanno degli effetti che si applicano a tutti i giocatori ed hanno la particolarità che rimangono attive fintanto che non viene pescata una nuova carta "Mercato" oppure che la carta attiva in quel momento sia scartata per effetto di un'altra carta. Le carte sostituite da una carta "Mercato" devono essere posizionate fuori dal gioco. Nel caso in cui il mazzo termini, tutte le carte "Mercato" scartate in precedenza vengono rimescolate assieme e andranno a comporre il nuovo mazzo. Un esempio di questa tipologia di carte è presente in Figura 4.7. Le carte "Mercato" hanno quindi la funzione di rendere l'ambiente di gioco più dinamico e imprevedibile, cercando di simulare i possibili cambiamenti che avvengono nel mondo reale in periodi temporali diversi. Questo rende il gioco meno ripetitivo e costringe i giocatori a rivedere la propria strategia durante il corso di una partita.

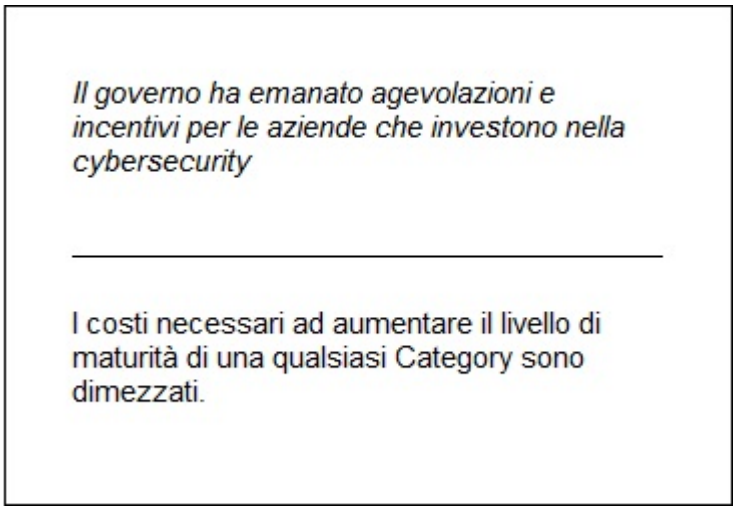

Fig. 4.7: Un esempio di carta Mercato

- **Casella Bonus Blu/Viola/Giallo/Rosso/Verde**: se la pedina termina su una delle tre caselle agli angoli del tabellone (esclusa la casella iniziale "Consiglio di Amministrazione"), il giocatore può

comportarsi come se fosse su una qualsiasi Category di uno dei due colori indicati dalla casella. Questo significa che, pagando il rispettivo costo, può decidere di aumentare il livello di maturità di una Category a sua scelta che appartenga ad uno dei colori indicati dalla casella bonus.

- **Casella Doppio Tiro**: se la pedina termina su una delle due caselle "Doppio Tiro" presenti, il giocatore ottiene un segnalino "Doppio Tiro" che consente al giocatore di tirare due volte il dado per spostarsi lungo il tabellone. Per utilizzare uno di questi segnalini, il giocatore deve dichiarare all'inizio del proprio turno (quindi prima di lanciare il dado) la sua intenzione a utilizzarlo. Una volta terminato il movimento, il segnalino viene scartato. Questa possibilità fa in modo che i giocatori che sono in possesso di tali segnalini possano raggiungere più rapidamente la zona della Function di cui hanno bisogno per avvicinarsi al proprio obiettivo e allo stesso tempo saltare quelle di cui si è già raggiunto il punteggio richiesto.

Se durante il movimento la pedina del giocatore dovesse attraversare o fermarsi sulla casella di partenza "Consiglio di Amministrazione", il giocatore percepisce dai vertici dell'organizzazione nuovi fondi che gli serviranno per continuare a mantenere ed espandere la qualità della sicurezza della propria azienda. In pratica, al giocatore vengono assegnati 100 euro per ogni transito su tale casella.
All'interno di Securopoly esistono anche i cosiddetti segnalini "Rischio": questi segnalini rappresentano dei malus che vengono assegnati ai giocatori solitamente quando non riescono a soddisfare le richieste di alcune carte "Imprevisto" o "Probabilità". Nella realtà, questi segnalini "Rischio" sono di fatto le vulnerabilità presenti all'interno dei sistemi informatici (e non) dell'azienda che possono essere sfruttate da gruppi di malintenzionati per arrecare danni economici, rubare dati sensibili dell'organizzazione o portare a termine altre attività illecite.
Quando un giocatore entra in possesso del suo terzo segnalino "Rischio", tale giocatore è automaticamente vittima di un attacco informatico e deve fare i conti immediatamente con l'incidente che interessa la sua azienda in quel momento. A seconda di quanto è alto il livello di maturità della Category "Contenimento e Mitigazione di un Incidente", questi generi di attacchi possono essere, appunto, mitigati.
I fattori rilevanti nel calcolo dei danni economici che il giocatore sarà costretto a pagare sono quindi il numero di segnalini "Rischio" in possesso del giocatore e il livello di maturità della Category sopra citata. In particolare, ogni segnalino vale 50 euro, mentre ogni livello di maturità dà il

diritto a scartare un segnalino "Rischio" prima del calcolo dei danni che il giocatore sarà costretto a pagare per rimediare all'incidente.
Facciamo un esempio: un giocatore possiede già due segnalini "Rischio" e pesca una carta "Imprevisto" che al termine del suo effetto gli assegna un altro segnalino. A questo punto il giocatore si ritrova con 3 segnalini "Rischio" e quindi è vittima di un attacco informatico. La Category "Contenimento e Mitigazione di un Incidente" è però al livello di maturità 2, cosa che permette al giocatore di scartare 2 segnalini prima di andare al conteggio dei danni. Il giocatore dovrà quindi pagare esclusivamente il valore di un singolo segnalino, cioè 50 euro.
Nel caso in cui un giocatore dovesse esaurire le risorse economiche a sua disposizione (sia in seguito ad un attacco informatico, sia attraverso effetti di altre carte), può richiedere per una sola volta durante la partita l'anticipo dei soldi che gli dovrebbero essere consegnati al passaggio dalla casella "Consiglio di Amministrazione". In questo modo, può concludere di pagare la somma che altrimenti non sarebbe riuscito a sostenere. Avendo però già ricevuto fondi aggiuntivi, la volta successiva che transiterà dalla casella iniziale non gli sarà consegnata la quota solitamente prevista.
Nel malaugurato caso che un giocatore, dopo aver già richiesto una volta un anticipo, termini nuovamente i fondi a sua disposizione, i vertici dell'organizzazione saranno costretti a sollevare il manager dal suo incarico e licenziarlo, eliminando così il giocatore dalla partita.

4.5 Conclusione

Siamo giunti alla parte finale di Securopoly, ovvero quali sono le condizioni di vittoria e in che modo termina una partita.
Molto semplicemente, vince il giocatore che per primo riesce a raggiungere per ogni Function i punteggi segnati nella propria carta "Profilo Target", aumentando il livello di maturità delle Category che ne fanno parte.
Nel caso però in cui uno o più giocatori dovessero essere eliminati dal gioco, la vittoria va all'ultimo giocatore rimasto in partita.

5. SIMULAZIONE DI UNA PARTITA

In questo capitolo è presente la simulazione della parte iniziale di una partita di Securopoly, partendo sin dalle fasi di preparazione del tabellone e delle carte fino ad arrivare ai movimenti veri e propri dei giocatori. In questa simulazione saranno mostrati tutte i possibili eventi che possono accadere durante il gioco.
La simulazione tratterà una partita composta da 3 giocatori chiamati semplicemente Andrea, Bianca e Claudio.
Innanzitutto ogni giocatore sceglie il colore della pedina e dei propri marcatori che lo rappresenteranno durante il corso del gioco. Andrea sceglie il colore Verde, Bianca sceglie il colore Rosso e Claudio sceglie il colore Blu. I giocatori posizionano poi le proprie pedine nella casella di partenza "Consiglio di Amministrazione" .
Si prendono ora tutte le carte "Profilo Attuale" che rappresentano l'insieme delle Category della propria azienda già in parte sviluppate e le si mescola assieme formando il relativo mazzo da cui ogni giocatore pesca una carta. Andrea legge la seguente situazione iniziale della sua azienda nella carta che ha pescato (mostrata in Figura 5.1):

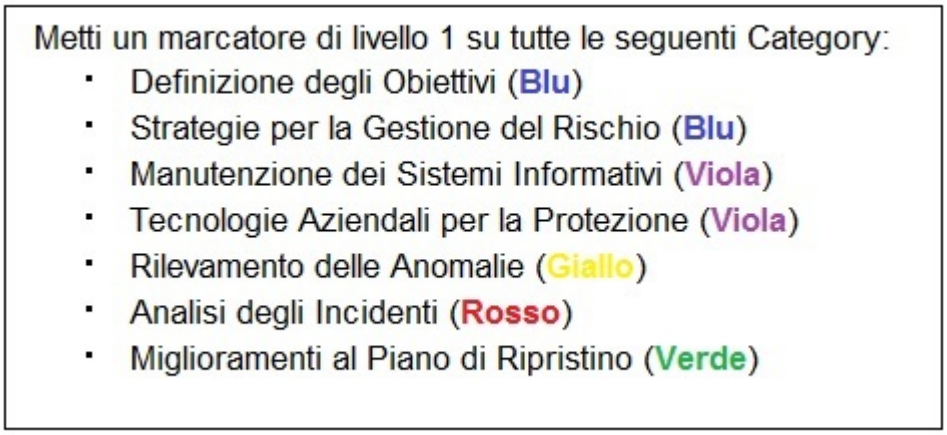

Fig. 5.1: La carta Profilo Attuale pescata da Andrea

- La Category Blu "Definizione degli Obiettivi" parte dal livello di maturità 1;
- La Category Blu "Strategia per la Gestione del Rischio" parte dal livello di maturità 1;
- La Category Viola "Manutenzione dei Sistemi Informativi" parte dal livello di maturità 1;
- La Category Viola "Tecnologie Aziendali per la Protezione" parte dal livello di maturità 1;
- La Category Gialla "Rilevamento delle Anomalie" parte dal livello di maturità 1;
- La Category Rossa "Analisi degli Incidenti" parte dal livello di maturità 1;
- La Category Verde "Miglioramenti al Piano di Ripristino" parte dal livello di maturità 1;

Seguendo le istruzioni fornite sulla carta, in questo caso Andrea posiziona su ogni casella elencata dal suo "Profilo Attuale" un marcatore del proprio colore di livello 1.
Lo stesso procedimento avviene ora per gli altri due giocatori.
Bianca legge la seguente situazione iniziale della sua azienda nella carta che ha pescato:

- La Category Blu "Definizione della Politica Aziendale per la Cybersecurity" parte dal livello di maturità 1;
- La Category Viola "Sicurezza dei Dati" parte dal livello di maturità 1;
- La Category Viola "Configurazione dei Sistemi Informativi" parte dal livello di maturità 1;
- La Category Gialla "Consistenza dei Processi di Rilevamento" parte dal livello di maturità 1;
- La Category Rossa "Coordinamento delle Operazioni di Risposta" parte dal livello di maturità 1;
- La Category Verde "Miglioramenti al Piano di Ripristino" parte dal livello di maturità 1;

Seguendo le istruzioni fornite sulla carta, Bianca posiziona su ogni casella elencata dal suo "Profilo Attuale" un marcatore del proprio colore di livello 1.
Claudio legge la seguente situazione iniziale della sua azienda nella carta che ha pescato:

- La Category Blu "Valutazione del Rischio" parte dal livello di maturità 1;
- La Category Viola "Controllo degli Accessi" parte dal livello di maturità 1;
- La Category Viola "Sicurezza dei Dati" parte dal livello di maturità 1;
- La Category Gialla "Monitoraggio dei Sistemi Informativi" parte dal livello di maturità 1;
- La Category Rossa "Miglioramenti al Piano di Risposta" parte dal livello di maturità 1;
- La Category Verde "Gestione delle Comunicazioni in seguito ad un Incidente" parte dal livello di maturità 1;

Seguendo le istruzioni fornite sulla carta, Claudio posiziona su ogni casella elencata dal suo "Profilo Attuale" un marcatore del proprio colore di livello 1.
A questo punto tutte le carte "Profilo Attuale" vengono messe da parte e non saranno più utilizzate nel corso della partita.
Ora vengono mischiate assieme le carte "Profilo Target" e ogni giocatore pesca una carta dall'interno di questo mazzo per scoprire i propri obiettivi per questa partita. Al contrario delle carte "Profilo Attuale", questa volta i giocatori non rivelano la carta pescata ma la conservano per sè.
Nella carta "Profilo Target" di Andrea (visibile in Figura 5.2), i punteggi totali delle 5 Function richiesti al giocatore sono:

- Totale livelli di maturità Blu: 7;
- Totale livelli di maturità Viola: 8;
- Totale livelli di maturità Giallo: 3;
- Totale livelli di maturità Rosso: 5;
- Totale livelli di maturità Verde: 2;

Fig. 5.2: La carta Profilo Target pescata da Andrea

Andrea possiede già di partenza due Category al livello di maturità 1 nella Function Blu quindi, ad esempio, per raggiungere il suo obiettivo di 7 punti deve riuscire ad aumentare di 5 livelli complessivi altre Category appartenenti alla Function "Identificare". Lo stesso ragionamento vale per tutte le altre Function. In questo caso, nella Function Viola Andrea possiede 2 punti, mentre in tutte le altre Function parte con 1 punto per ognuna.
Nella carta "Profilo Target" di Bianca, i punteggi totali delle 5 Function richiesti al giocatore sono:

- Totale livelli di maturità Blu: 6;
- Totale livelli di maturità Viola: 9;
- Totale livelli di maturità Giallo: 3;
- Totale livelli di maturità Rosso: 5;
- Totale livelli di maturità Verde: 2;

B possiede un punteggio pari a 1 in tutte le Category tranne quella Viola, dove parte con 2 punti. Nella carta "Profilo Target" di Claudio, i punteggi totali delle 5 Function richiesti al giocatore sono:

- Totale livelli di maturità Blu: 5;
- Totale livelli di maturità Viola: 10;

- Totale livelli di maturità Giallo: 4;
- Totale livelli di maturità Rosso: 4;
- Totale livelli di maturità Verde: 2;

Come Bianca, anche Claudio parte con un punteggio pari a 1 in tutte le Category tranne quella Viola, dove ha 2 punti.
Può sembrare da questo particolare caso che Andrea parta avvantaggiato rispetto agli altri due giocatori avendo un punto di partenza in più nella Function "Identificare". In realtà, le Category assegnate ad Andrea sono anche le meno influenti per tale Function, essendo caselle che possono essere "potenziate" solo fino al livello di maturità 1. Infatti, le Category più importanti e che hanno un impatto maggiore nel corso della partita sono quelle di cui è possibile aumentare il relativo livello di maturità fino a 3. Questa caratteristica è basata sul fatto che, all'interno del Framework Nazionale, le Category hanno livelli di priorità diversi (a seconda delle SubCategory che le compongono) e questo è ripreso in Securopoly dando a tali caselle più possibili livelli di maturità e in generale una importanza maggiore (ad esempio quante volte tali Category sono utilizzate dalle carte Imprevisto/Probabilità).
A questo punto, le rimanenti carte "Profilo Target" vengono messe da parte. Si prendono ora le carte Imprevisto, Probabilità e Mercato e si formano i tre mazzi corrispondenti che, dopo averli mescolati, si posizionano nel loro relativo spazio sul tabellone.
A tutti i giocatori vengono distribuiti 200 euro come fondi di partenza assegnati dalle proprie organizzazioni.
Per terminare la fase di preparazione della partita, ogni giocatore tira il dado e chi fa il numero più alto partirà per primo. In seguito, il gioco prosegue in senso orario. Andrea tira il dado e ottiene 3, il risultato del tiro di Bianca è 2 mentre quello di Claudio è 5, quindi sarà lui a partire per primo.
Riassumendo, la situazione sul tabellone prima dell'inizio vero e proprio della partita è rappresentata in Figura 5.3.

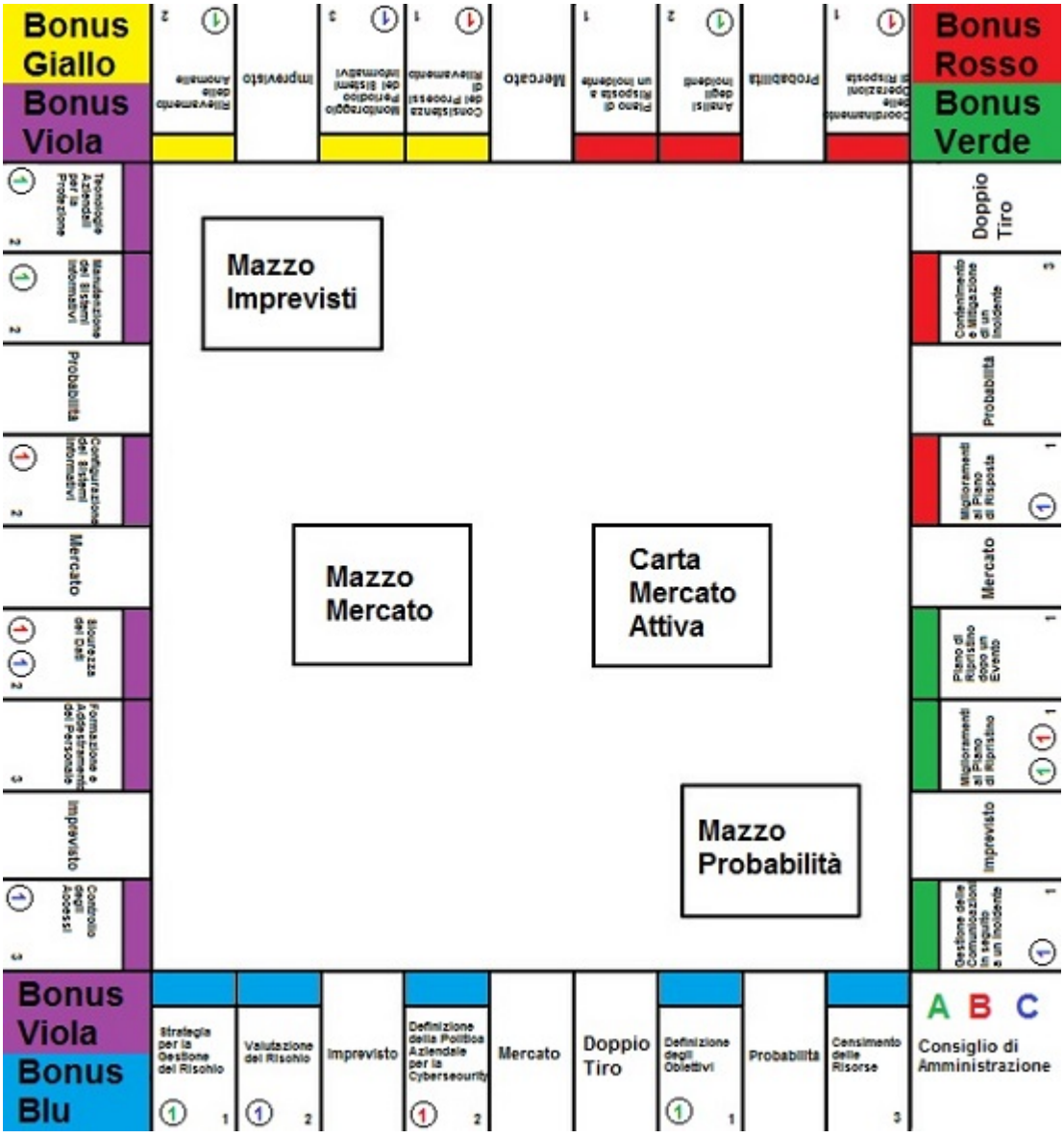

Fig. 5.3: Rappresentazione del Tabellone dopo la fase di preparazione della partita

1° turno di Claudio: Claudio tira il dado e ottiene 4. La sua pedina termina su una casella "Doppio Tiro". Claudio guadagna un segnalino "Doppio Tiro" che potrà utilizzare in un prossimo turno. Il gioco passa ora ad Andrea.
1° turno di Andrea: Andrea tira e ottiene 5. Finisce quindi su una casella "Mercato". Pesca una carta dal relativo mazzo il cui effetto è quello di dimezzare tutti i costi per aumentare i livelli di maturità di ogni Category. Andrea posiziona la carta "Mercato" attiva nell'apposito spazio. Il suo turno è concluso.
1° turno di Bianca: Bianca tira il dado e ottiene 3. Arriva sulla Category "Definizione degli Obiettivi" e decide di investire una parte dei suoi fondi per aumentare il livello di maturità di tale casella a 1. È ininfluente ai fini del gioco che in tale casella sia già presente il marcatore di Andrea, infatti si ricorda che le Category sono condivise da ogni giocatore al contrario di quanto avviene per le caselle del Monopoly classico. Nel turno precedente però, Andrea aveva attivato la carta "Mercato" che permetteva di investire la metà dei soldi solitamente utilizzati per aumentare i livelli di maturità di tutte le Category. Bianca quindi paga 10 euro (riponendoli assieme alle altre banconote non utilizzate) al posto di 20 e posiziona uno dei suoi marcatori di livello 1 sulla casella dove si trova. Bianca quindi sa che ora le mancano altri 4 punti per raggiungere il suo obiettivo di 6 punti totali nella Function Blu.
Al termine del primo giro, la situazione aggiornata del tabellone è mostrata in Figura 5.4.

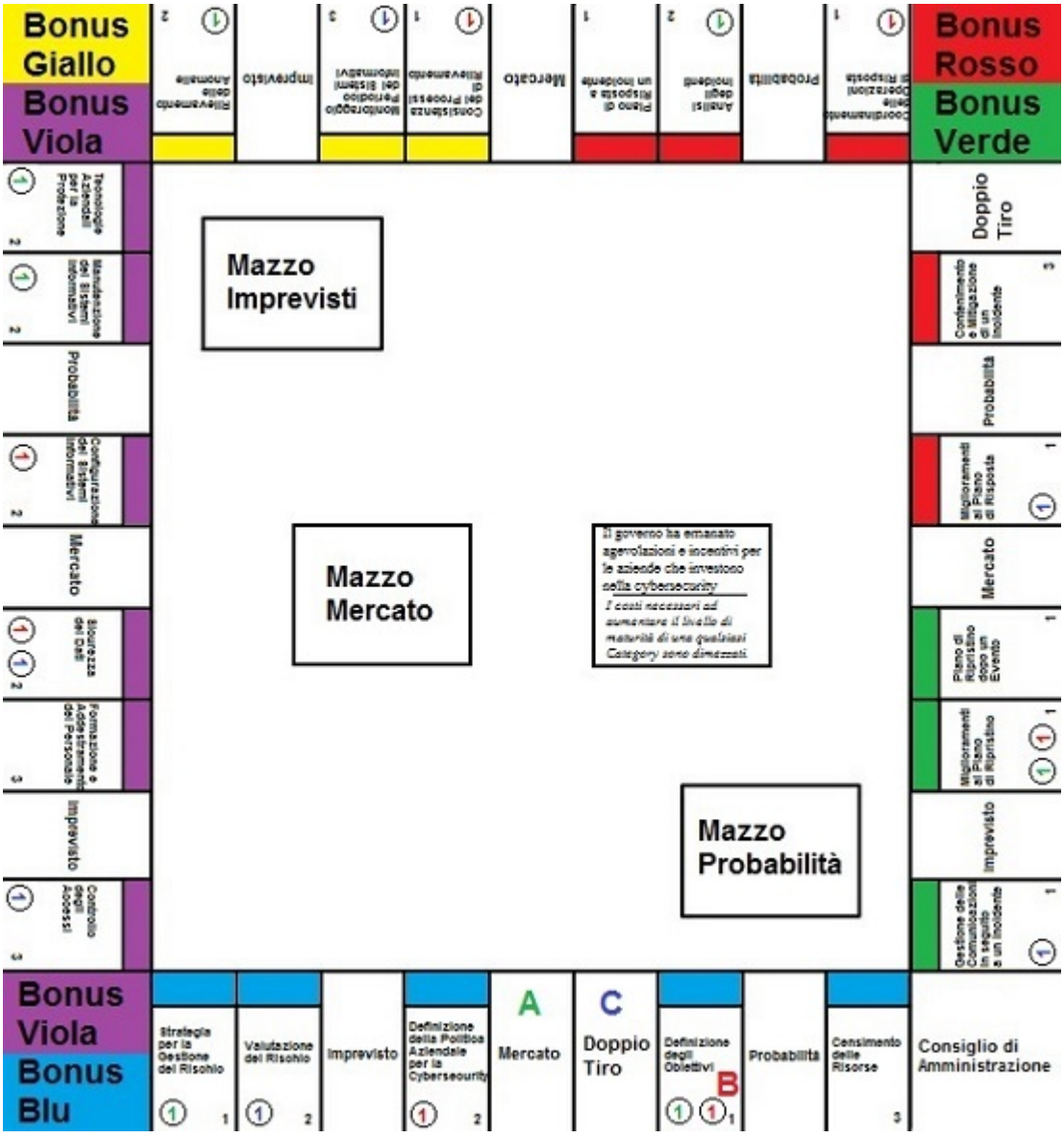

Fig. 5.4: Rappresentazione del Tabellone dopo i primi 3 turni

2° turno di Claudio: Claudio ottiene un 6 dal lancio del dado e arriva sulla casella Bonus Blu/Viola. Questa casella dà il diritto al giocatore di decidere a proprio piacimento una Category appartenente a uno dei due colori specificati e aumentare il suo livello di maturità pagando la somma necessaria. Tutte le caselle Bonus quindi danno la possibilità al giocatore di investire in una particolare Category desiderata che magari non si è riusciti a migliorare nei turni precedenti. In questo caso Claudio sceglie la Category Blu "Censimento delle Risorse" e, sempre grazie alla carta "Mercato" attiva, paga 10 euro per portarla al livello di maturità 1.
2° turno di Andrea: Andrea fa 4 con il dado e arriva sulla Category Blu "Strategia per la Gestione del Rischio" che lui possiede già al livello di maturità 1. Dato che tale Category è già potenziata al massimo, Andrea riceve 10 euro e ha la possibilità di potenziare una qualsiasi altra Category appartenente alla Function "Identificare". Andrea sceglie di investire i 10 euro appena ottenuti per aumentare al livello di maturità 1 la Category Blu "Censimento delle Risorse" (essendo la casella più importante della Function Blu) come ha fatto nel turno precedente Claudio.
2° turno di Bianca: Anche Bianca ottiene un 4 dal dado e finisce su una casella "Imprevisto". Bianca pesca una carta dal relativo mazzo e ottiene la carta in Figura 5.5. Bianca non possiede il livello di maturità richiesto nella

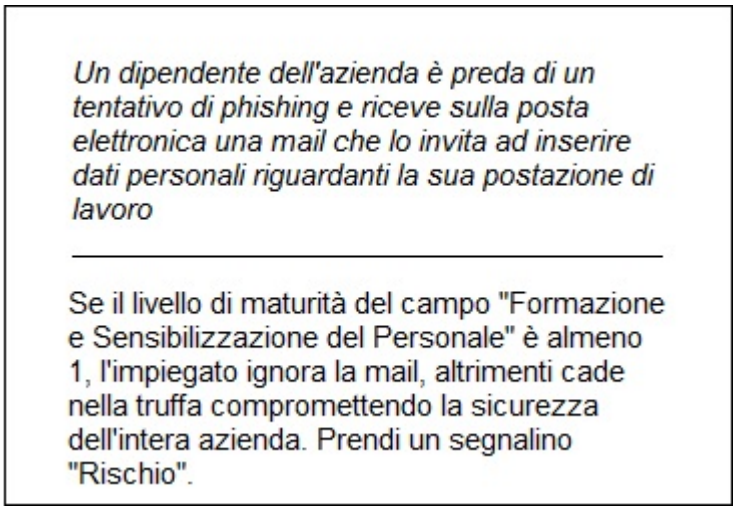

Fig. 5.5: La carta Imprevisto pescata da Bianca

Category menzionata dalla carta Imprevisto, quindi è costretta a prendere un segnalino "Rischio" e concludere il proprio turno.
Al termine del secondo giro, la situazione aggiornata del tabellone è mostrata in Figura 5.6. Inoltre, fino a questo momento, Andrea possiede ancora 200

euro, Bianca ha 190 euro e un segnalino "Rischio", mentre Claudio ha 190 euro e un segnalino "Doppio Tiro".

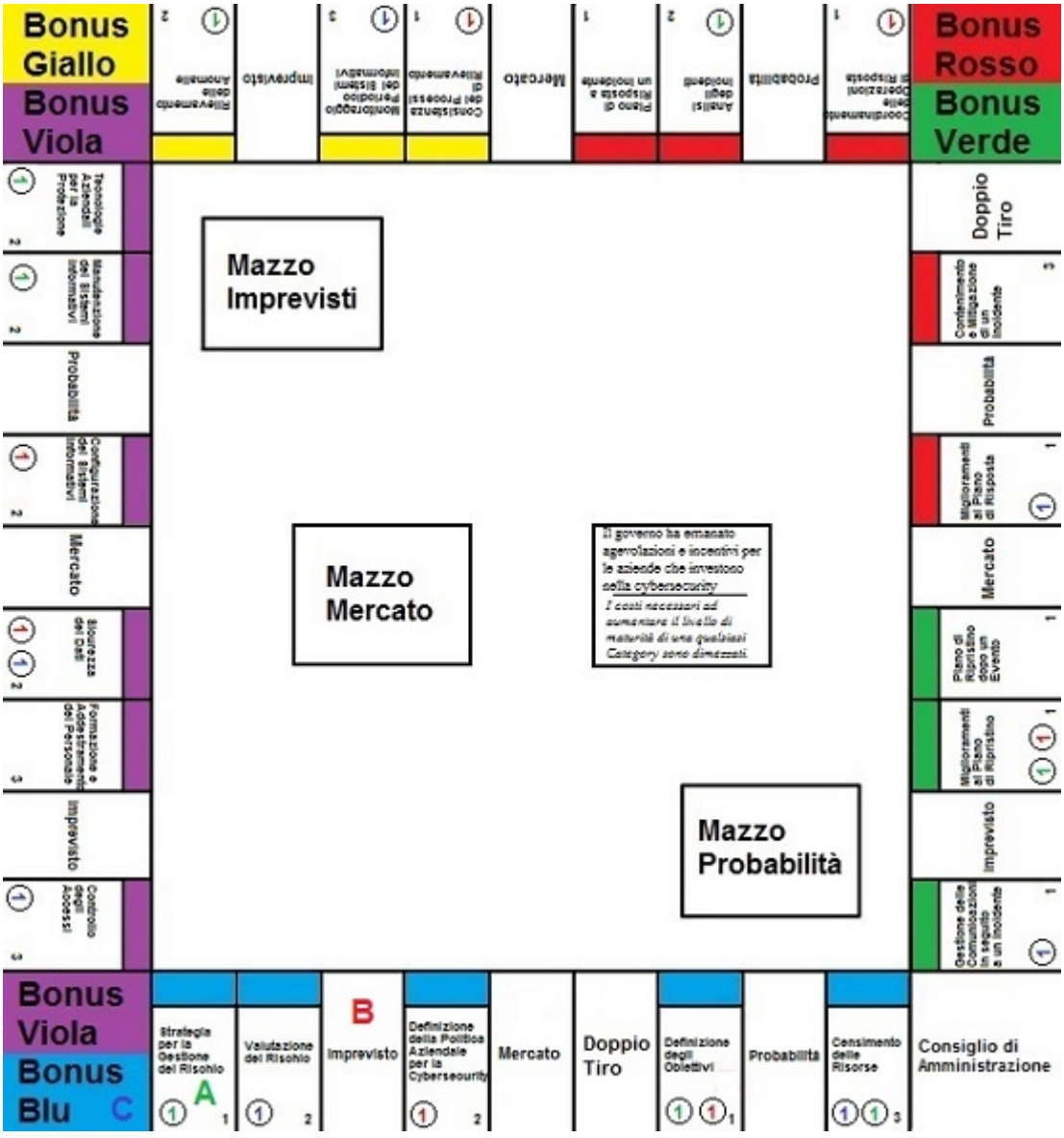

Fig. 5.6: Rappresentazione del Tabellone dopo il secondo giro

3° turno di Claudio: Claudio ottiene 1 dal dado e si muove sulla casella "Controllo degli Accessi". Claudio possiede già al livello di maturità 1 tale Category ma questa è potenziabile fino al livello 3, quindi decide di investire una parte dei suoi fondi per portare tale casella al livello 2. Sfruttando sempre la carta "Mercato" attiva, Claudio paga 20 euro e sostituisce il suo marcatore presente sulla casella con uno di livello 2.
3° turno di Andrea: Andrea fa 6 con il dado e arriva su una casella "Mercato". Essendoci già una carta "Mercato" attiva, Andrea la ripone fuori dal gioco e ne pesca una nuova il cui effetto è quello di trasformare tutte le caselle "Probabilità" in caselle "Imprevisto" fintanto che tale carta rimane attiva.
3° turno di Bianca: Bianca ottiene 6 dal lancio del dado. Si muove sulla Category "Formazione e Addestramento del Personale" e vede che è una casella il cui livello di maturità può arrivare fino a 3, ciò significa che è una Category importante del Framework Core e del gioco in sè. Decide quindi di pagare 20 euro e di portare tale casella al livello di maturità 1.
Al termine del terzo giro, la situazione aggiornata del tabellone è mostrata in Figura 5.7.

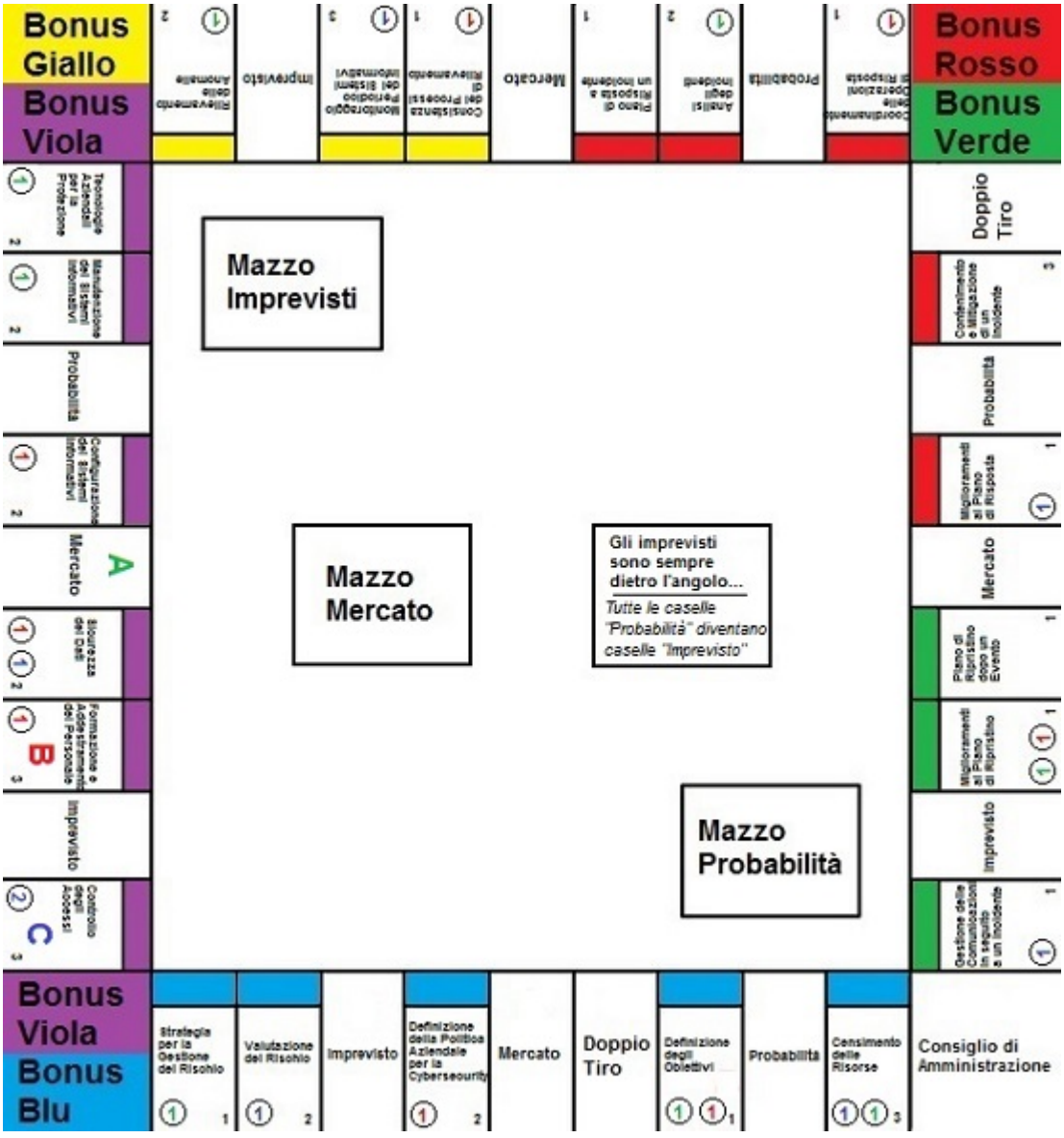

Fig. 5.7: Rappresentazione del Tabellone dopo il terzo giro

4° turno di Claudio: Claudio tira il dado e ottiene 6. Si muove su una casella "Probabilità" che però, per effetto della carta "Mercato" attiva, viene trasformata in una casella "Imprevisto". Claudio pesca quindi una carta dal relativo mazzo che richiede al giocatore di avere la Category "Controllo degli Accessi" almeno al livello di maturità 1, ovvero richiede che all'interno dell'azienda vi sia un controllo generalizzato per garantire l'applicazione omogenea di regole minime di sicurezza. Claudio possiede tale Category al livello 2, quindi è in grado di soddisfare le richieste della carta "Imprevisto" e non incorrere nella sua penalità.
4° turno di Andrea: Andrea fa 6 con il dado e arriva sulla Category "Rilevamento delle Anomalie" che possiede già al livello di maturità 1. La casella può arrivare al massimo fino al livello 2, quindi Andrea decide di aumentarla al massimo investendo 40 euro e posiziona un suo marcatore di livello 2 al posto di quello di livello 1. In questo modo, oltre ad aumentare il proprio punteggio della Function "Rilevare", nel caso nei prossimi giri si fermasse ancora su tale casella potrebbe riscuotere un bonus e ampliare ulteriormente una delle altre Category Gialle a scelta.
4° turno di Bianca: Bianca ottiene 3 dal lancio del dado e termina sulla Category "Configurazione dei Sistemi Informativi". Decide anche lei, in modo simile a quello fatto da Andrea nel suo turno, di portare al massimo livello di maturità tale casella e pagare 40 euro per posizionare un suo marcatore di livello 2.
Al termine del quarto giro, la situazione aggiornata del tabellone è mostrata in Figura 5.8. Inoltre, fino a questo momento, Andrea possiede 160 euro, Bianca ha 130 euro e un segnalino "Rischio", mentre Claudio ha 170 euro e un segnalino "Doppio Tiro".

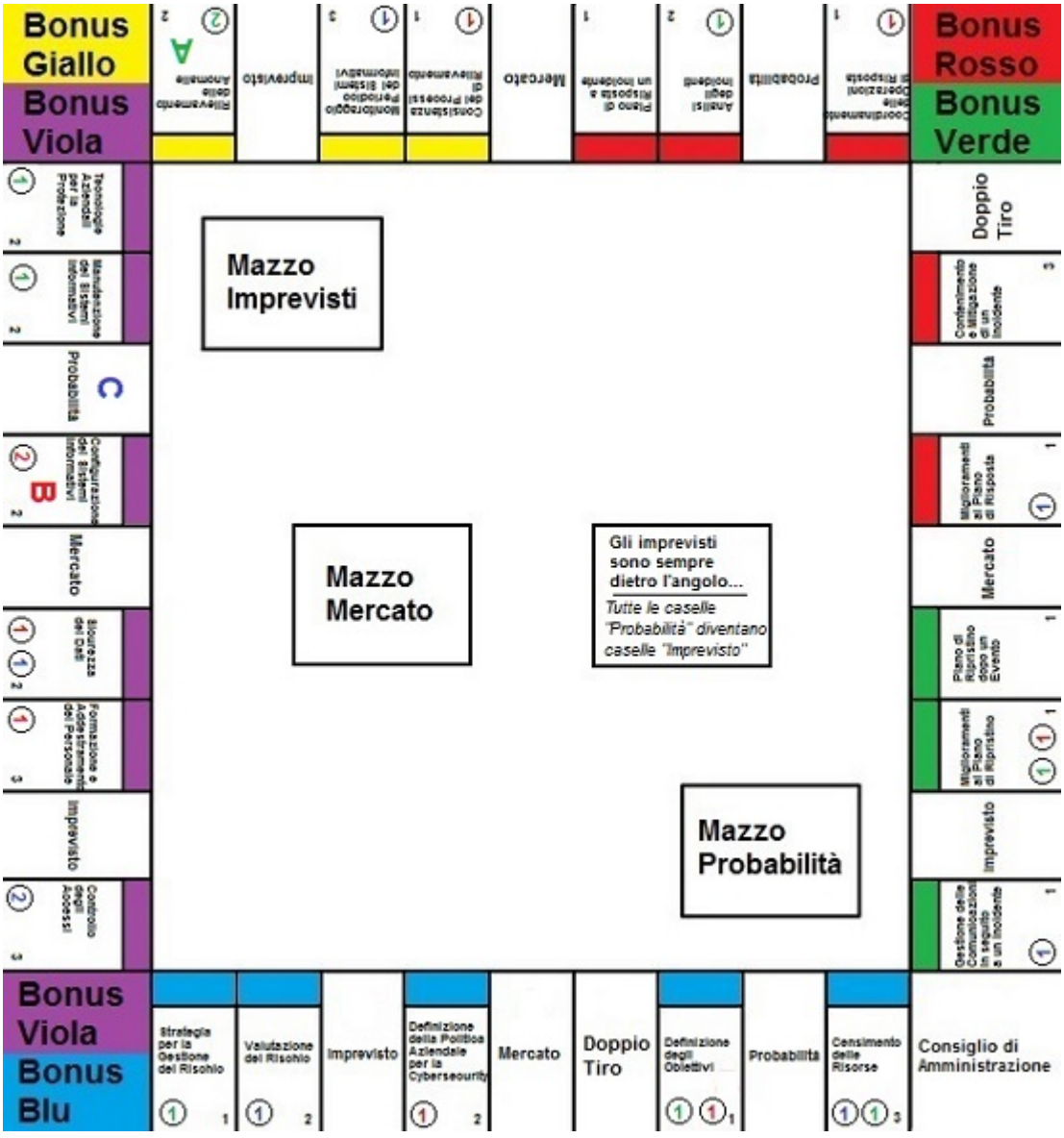

Fig. 5.8: Rappresentazione del Tabellone dopo il quarto giro

5° turno di Claudio: Claudio lancia il dado e fa 4. Arriva così alla Category "Rilevamento delle Anomalie" e decide di spendere 20 euro per alzare il livello di maturità di tale casella a 1. Posiziona quindi un suo marcatore di tale livello e conclude il suo turno.
5° turno di Andrea: Andrea ottiene 3 dal lancio del dado e si muove nella casella che rappresenta la Category "Consistenza dei Processi di Rilevamento". Andrea riguarda la sua carta "Profilo Target" e nota che il punteggio che gli viene richiesto per quanto riguarda la Function "Rilevare" è pari a 3. Questo vuol dire che aumentando di uno il livello di maturità della casella su cui è capitato in questo turno raggiungerebbe il punteggio indicato dal suo obiettivo, dato che possiede già 2 punti dati dalla Category "Rilevamento delle Anomalie" portata al livello di maturità 2 nel turno precedente. Per questo motivo Andrea decide di pagare 20 euro e posiziona un suo marcatore sulla casella occupata. Andrea ha così completato una parte del suo obiettivo per quanto riguarda la Function Gialla e nel corso dei prossimi giri non sarà più necessario per lui dover spendere risorse per incrementare il livello delle caselle Gialle.
5° turno di Bianca: Bianca ottiene 6 dal lancio del dado e arriva ancora su una casella "Imprevisto". Pesca una carta dal relativo mazzo che le richiede di avere la Category "Tecnologie Aziendali per la Protezione" almeno al livello 1 per fare in modo che il firewall aziendale sia abbastanza sofisticato da bloccare tentativi di connessione non autorizzati. Purtroppo Bianca non possiede tale livello di maturità in quella Category quindi è costretta anche in questo caso a prendere un secondo segnalino "Rischio".
Al termine del quinto giro, la situazione aggiornata del tabellone è mostrata in Figura 5.9. Inoltre, fino a questo momento, Andrea possiede 140 euro, Bianca ha 130 euro e due segnalini "Rischio", mentre Claudio ha 150 euro e un segnalino "Doppio Tiro".

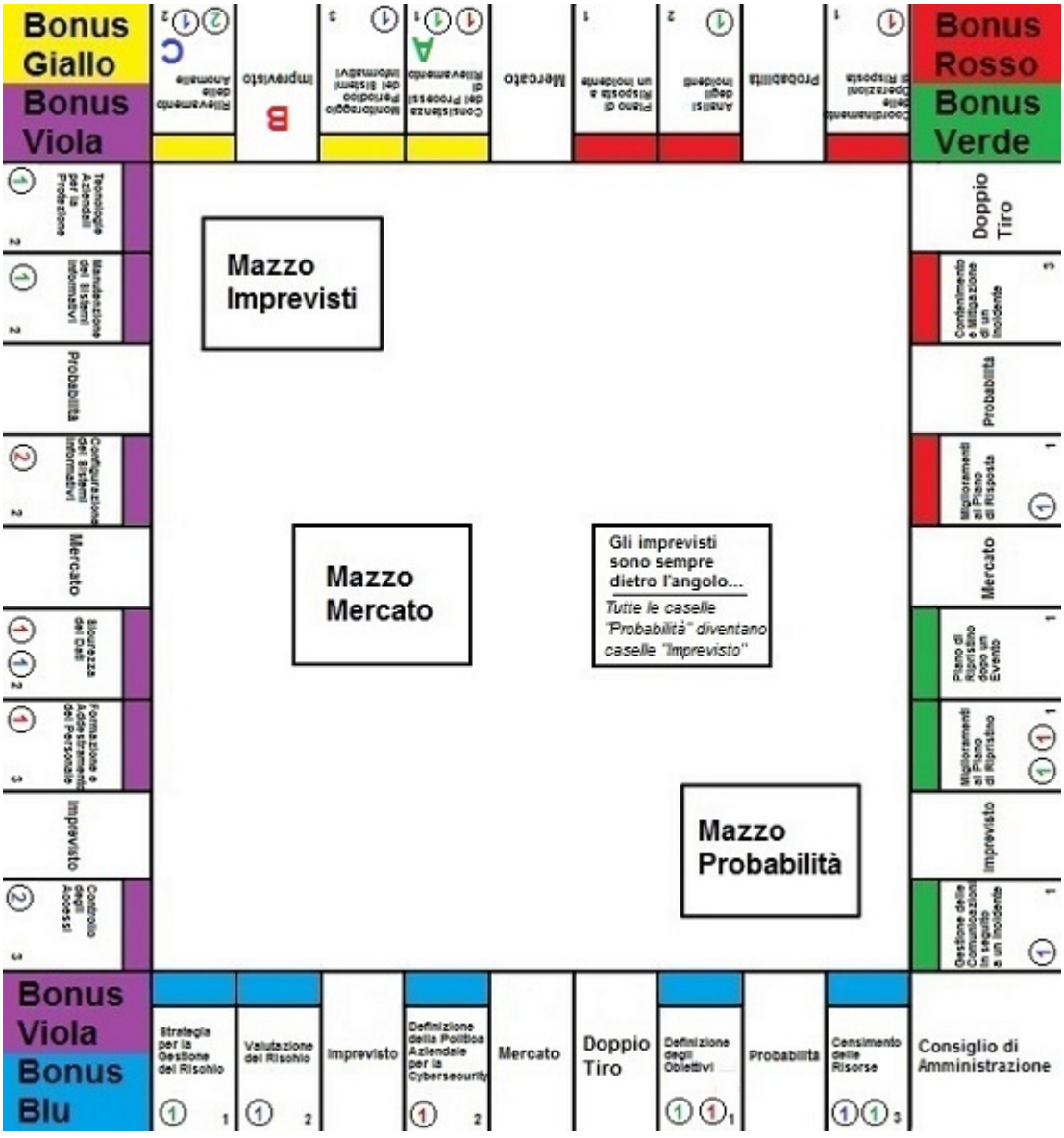

Fig. 5.9: Rappresentazione del Tabellone dopo il quinto giro

6° turno di Claudio: Claudio tira il dado e ottiene un 6. Arriva così alla Category "Analisi degli Incidenti". Avendo ancora abbastanza fondi da investire, Claudio decide di pagare 20 euro e posiziona un marcatore di livello 1 su tale casella.
6° turno di Andrea: Andrea ottiene un 2 dal lancio del dado e termina sulla casella "Piano di Risposta a un Incidente". Paga 20 euro per poter aumentare a 1 il livello di maturità di tale Category e avvicinarsi così di un punto al suo obiettivo per quanto riguarda la Function Rossa.
6° turno di Bianca: Bianca ottiene un 3 e arriva su una casella "Mercato". Pesca una carta dal relativo mazzo che ha il solo effetto di dare istantaneamente un segnalino "Rischio" a tutti i giocatori. Claudio e Andrea ottengono così il loro primo segnalino di questo tipo, mentre Bianca arriva a quota 3 segnalini. Avendo accumulato così tante vulnerabilità all'interno della sua organizzazione, Bianca è vittima di un attacco informatico e deve affrontare immediatamente le conseguenze di questo evento. Si ricorda che ogni segnalino "Rischio" vale 50 euro e che ogni livello di maturità della Category "Contenimento e Mitigazione di un Incidente" permette di scartare un segnalino dal calcolo dei danni. Bianca però non possiede nemmeno il livello 1 di tale Category, quindi sarà costretta a pagare per intero il valore dei 3 segnalini "Rischio". In totale Bianca ha ancora tra i suoi fondi 130 euro che però non sono sufficienti per pagare gli interi danni economici provocati dall'attacco informatico, e deve quindi richiedere un anticipo dei soldi che gli verrebbero consegnati durante il passaggio dalla casella di partenza "Consiglio di Amministrazione". Bianca utilizza quindi una parte dei 100 euro ricevuti in questo modo per concludere il suo debito. Avendo ottenuto questo prestito, la prossima volta che Bianca transiterà sulla casella iniziale non potrà ottenere i fondi che le spetterebbero. Alla fine del calcolo dei danni e del pagamento, Bianca scarta tutti i suoi segnalini "Rischio". Nel malaugurato caso che Bianca dovesse finire i soldi una seconda volta, non potrebbe più richiedere un prestito e quindi dovrà essere licenziata dai piani della sua azienda ed eliminata dal gioco.
Al termine del sesto giro, la situazione aggiornata del tabellone è mostrata in Figura 5.10. Inoltre, fino a questo momento, Andrea possiede 120 euro e un segnalino "Rischio", Bianca ha 80 euro ed ha già richiesto il prestito, mentre Claudio ha 130 euro, un segnalino "Rischio" e un segnalino "Doppio Tiro".

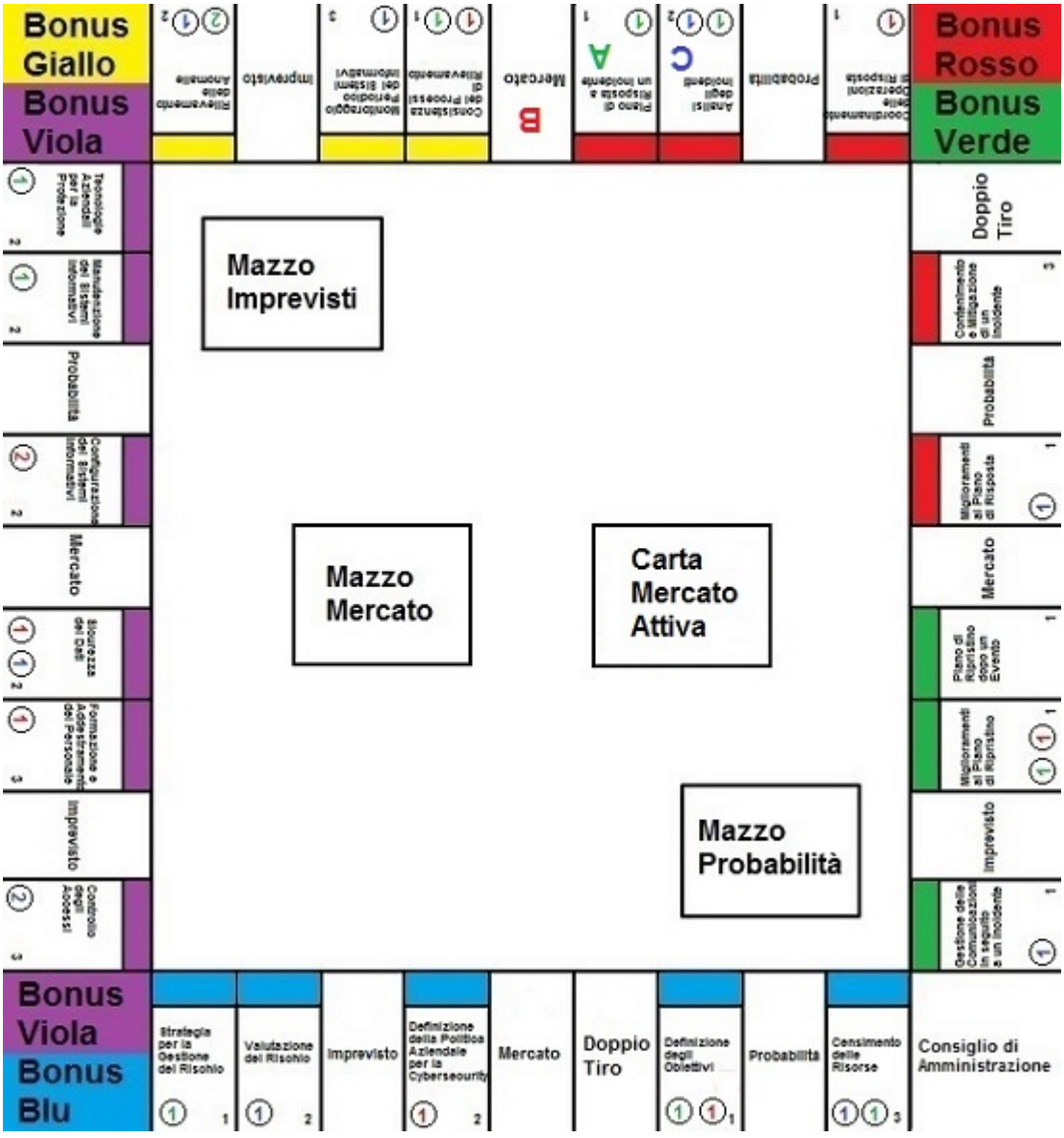

Fig. 5.10: Rappresentazione del Tabellone dopo il sesto giro

7° turno di Claudio: all'inizio del suo turno, Claudio annuncia di voler utilizzare il proprio segnalino "Doppio Tiro" che gli permette di tirare due volte il dado e sommare i punteggi ottenuti per muoversi più velocemente lungo il tabellone e raggiungere in meno tempo la casella iniziale e ricevere ulteriori fondi a sua disposizione. Claudio tira quindi due volte il dado e ottiene un 4 e un 5, raggiungendo così la Category "Piano di Ripristino dopo un Evento". Paga 20 euro per poter aumentare tale Category al livello di maturità 1 e posiziona il rispettivo marcatore sulla casella occupata. Nel prossimo turno gli basterà ottenere almeno un 4 per raggiungere il suo scopo e arrivare nella casella "Consiglio di Amministrazione" e ricevere i fondi aggiuntivi.
7° turno di Andrea: Andrea tira il dado e ottiene un 2. Termina su una casella "Probabilità" e pesca una carta dal relativo mazzo. Su quest'ultima si legge che se la Category "Rilevamento delle Anomalie" è almeno al livello di maturità 2, i sensori in uso rilevano, appunto, un'attività anomala nei sistemi dell'azienda e avvisano i responsabili, i quali riescono a gestirla per tempo. Andrea riesce a soddisfare i requisiti della carta dato che possiede tale Category al livello 2 come richiesto e per questo la carta lo premia dandogli la possibilità di scartare un segnalino "Rischio" posseduto. Andrea quindi rimette a posto il segnalino e termina il suo turno.
7° turno di Bianca: Bianca ottiene un 1 dal lancio del dado. Si muove sulla Category "Piano di Risposta a un Incidente" ma decide di non investire i suoi soldi per aumentare il livello di maturità di tale casella. Non avendo molti fondi a sua disposizione e avendo già richiesto un prestito, preferisce aspettare un'altra occasione nei prossimi giri quando avrà riottenuto un budget maggiore e non rischiare di essere eliminata dal gioco precocemente.
Al termine del settimo giro, la situazione aggiornata del tabellone è mostrata in Figura 5.11. Inoltre, fino a questo momento, Andrea possiede 120 euro, Bianca ha 80 euro ed ha già richiesto il prestito, mentre Claudio ha 110 euro e un segnalino "Rischio".

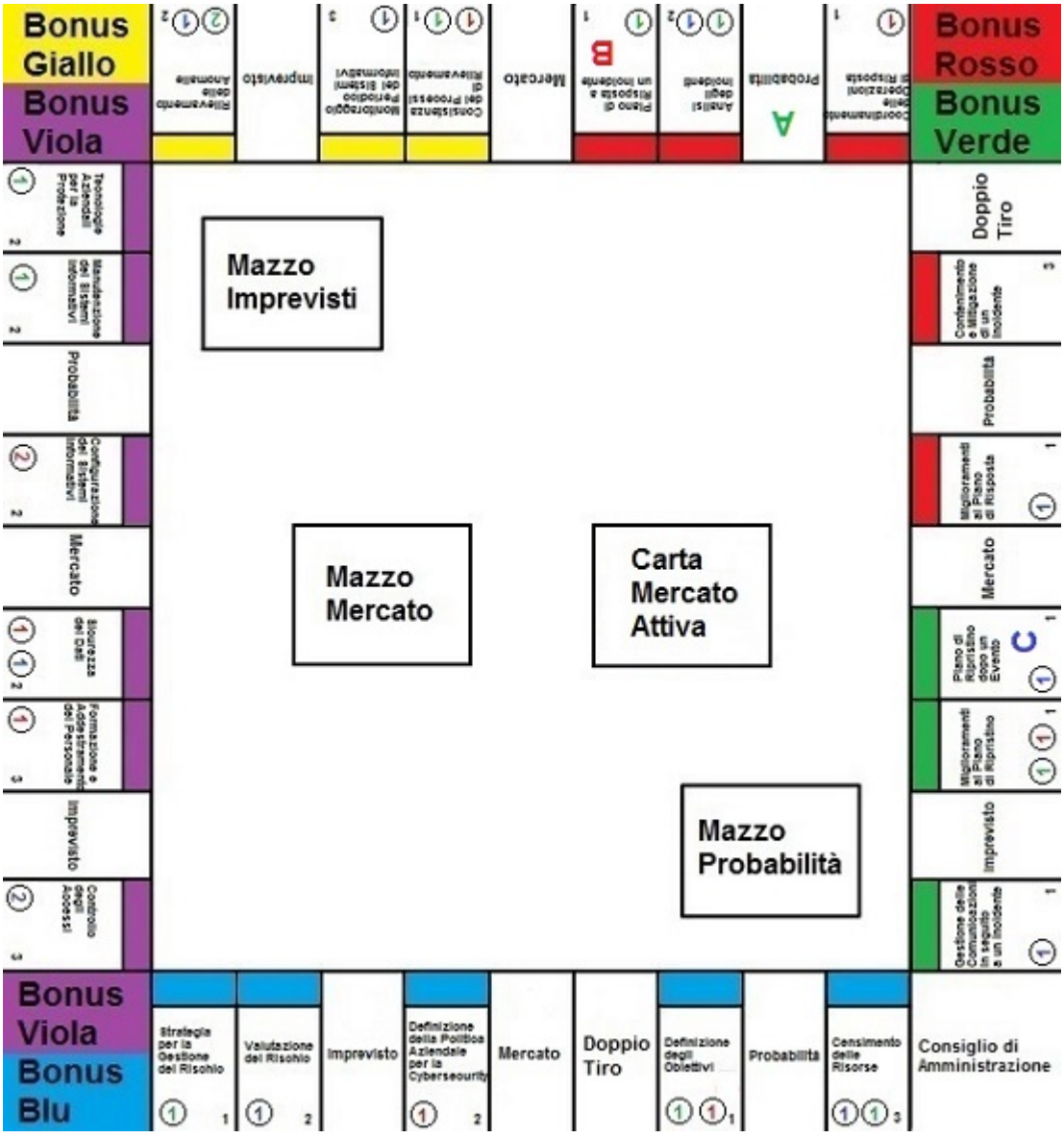

Fig. 5.11: Rappresentazione del Tabellone dopo il settimo giro

Il gioco ora prosegue fintanto che uno dei giocatori non raggiunge l'obiettivo presente sulla propria carta "Profilo Target" vincendo la partita, oppure termina nel caso dovesse rimanere un solo giocatore a causa dell'eliminazione di tutti gli altri. In quest'ultimo caso, l'ultimo giocatore rimasto diventa il vincitore.

6. CONCLUSIONI FINALI

All'interno di questa tesi è stata presentata la situazione odierna della cybersecurity e della sua diffusione. Abbiamo visto che le principali vulnerabilità all'interno di sistemi informativi sono causate da disattenzioni degli utenti che li utilizzano. La necessità primaria, quindi, è quella di istruire queste persone in modo tale che abbiano una conoscenza maggiore su temi riguardanti la sicurezza degli strumenti tecnologici che sono abituati ad adoperare.
Oltre ai programmi tradizionali, è stata presentata la gamification come strumento per rendere l'apprendimento più interattivo e rendere così l'esperienza più appagante agli occhi di un utente.
Sono stati descritti anche esempi esistenti di videogiochi e piattaforme che utilizzano la gamification per migliorare le capacità e le conoscenze di tutte le persone che si approcciano a questo tipo di apprendimento. Detto ciò, questi servizi non possono essere considerati validi per la totalità degli utenti interessati a migliorare le proprie conoscenze di sicurezza informatica perchè, ad esempio, non tutte le persone sono attirate dai videogiochi o da piattaforme online dedicate all'istruzione.
Da questi motivi nasce Securopoly, un gioco di società basato sul Framework Nazionale per la cybersecurity. A questo punto, è stato pertanto introdotto il Framework e sono state presentate tutte le caratteristiche che sono state riprese e adattate all'interno del gioco finale, come per esempio le Function e le Category del Framework Core, i livelli di Priorità e di Maturità e i Profili Attuali e Target.
Dopo aver quindi spiegato la struttura e gli strumenti offerti dal Framework Nazionale, sono state elencate le regole vere e proprie di Securopoly, spiegando dapprima al giocatore lo scopo del gioco e quali obiettivi deve cercare di soddisfare per raggiungere la vittoria finale. In seguito, viene fornito ai lettori l'elenco completo dei componenti che fanno parte di Securopoly. A questo punto, viene spiegata passo per passo la preparazione di una partita, come ad esempio la distribuzione delle carte per ogni giocatore e il posizionamento corretto dei marcatori appartenenti ai giocatori all'interno del tabellone di gioco. Infine, sono mostrate una per una le azioni possibili che i giocatori possono intraprendere durante il gioco

vero e proprio e i vari eventi che possono capitare a seconda della casella di arrivo di un giocatore, fino ai modi in cui la partita termina e viene proclamato il vincitore finale.
Come ultimo capitolo, viene poi mostrata un'ampia simulazione delle fasi iniziali di una partita, in modo tale che il lettore possa vedere un'applicazione diretta e pratica delle regole generali che ha appena visionato.
Per quanto mi riguarda, ho voluto creare Securopoly perchè credo che sia importante che esistano tanti modi diversi grazie ai quali le persone possano prendere coscienza delle problematiche sempre più attuali che interessano la sicurezza informatica, per questo un gioco di società può essere un ulteriore strumento in grado di avvicinare e istruire un maggior numero di utenti sui temi della cybersecurity.
La gamification è uno strumento fondamentale per rendere l'apprendimento più interessante e anche di qualità migliore, infatti negli ultimi anni è una tecnica che sta diventando sempre più importante e utilizzata in molti ambiti istruttivi diversi.
Infine, il fatto che Securopoly sia basato su un documento attuale come il Framework Nazionale per la cybersecurity lo rende uno strumento utilizzabile da tutte quelle organizzazioni che già seguono i concetti e le linee guida espresse in tale documento.

7. APPENDICI

7.1 Appendice A: Carte "Profilo Attuale" e "Profilo Target"

Questo è l'elenco di tutte le carte "Profilo Attuale" presenti nel gioco:

- Metti un marcatore di livello 1 su tutte le seguenti Category:
  - Definizione degli Obiettivi (Blu)
  - Strategie per la Gestione del Rischio (Blu)
  - Manutenzione dei Sistemi Informativi (Viola)
  - Tecnologie Aziendali per la Protezione (Viola)
  - Rilevamento delle Anomalie (Giallo)
  - Analisi degli Incidenti (Rosso)
  - Miglioramenti al Piano di Ripristino (Verde)
- Metti un marcatore di livello 1 su tutte le seguenti Category:
  - Definizione della Politica Aziendale per la Cybersecurity (Blu)
  - Sicurezza dei Dati (Viola)
  - Configurazione dei Sistemi Informativi (Viola)
  - Consistenza dei Processi di Rilevamento (Giallo)
  - Coordinamento delle Operazioni di Risposta (Rosso)
  - Miglioramenti al Piano di Ripristino (Verde)
- Metti un marcatore di livello 1 su tutte le seguenti Category:
  - Valutazione del Rischio (Blu)
  - Formazione e Addestramento del Personale (Viola)
  - Configurazione dei Sistemi Informativi (Viola)
  - Rilevamento delle Anomalie (Giallo)
  - Piano di Risposta a un Incidente (Rosso)

  - Miglioramenti al Piano di Ripristino (Verde)

- Metti un marcatore di livello 1 su tutte le seguenti Category:
  - Censimento delle Risorse (Blu)
  - Formazione e Addestramento del Personale (Viola)
  - Tecnologie Aziendali per la Protezione (Viola)
  - Consistenza dei Processi di Rilevamento (Giallo)
  - Piano di Risposta a un Incidente (Rosso)
  - Miglioramenti al Piano di Ripristino (Verde)
- Metti un marcatore di livello 1 su tutte le seguenti Category:
  - Definizione degli Obiettivi (Blu)
  - Strategie per la Gestione del Rischio (Blu)
  - Controllo degli Accessi (Viola)
  - Manutenzione dei Sistemi Informativi (Viola)
  - Rilevamento delle Anomalie (Giallo)
  - Coordinamento delle Operazioni di Risposta (Rosso)
  - Gestione delle Comunicazioni in seguito a un Incidente (Verde)
- Metti un marcatore di livello 1 su tutte le seguenti Category:
  - Definizione della Politica Aziendale per la Cybersecurity (Blu)
  - Controllo degli Accessi (Viola)
  - Configurazione dei Sistemi Informativi (Viola)
  - Rilevamento delle Anomalie (Giallo)
  - Miglioramenti al Piano di Risposta (Rosso)
  - Gestione delle Comunicazioni in seguito a un Incidente (Verde)
- Metti un marcatore di livello 1 su tutte le seguenti Category:
  - Valutazione del Rischio (Blu)
  - Controllo degli Accessi (Viola)
  - Sicurezza dei Dati (Viola)
  - Monitoraggio Periodico dei Sistemi Informativi (Giallo)
  - Miglioramenti al Piano di Risposta (Rosso)

  - Gestione delle Comunicazioni in seguito a un Incidente (Verde)

- Metti un marcatore di livello 1 su tutte le seguenti Category:
  - Censimento delle Risorse (Blu)
  - Controllo degli Accessi (Viola)
  - Tecnologie Aziendali per la Protezione (Viola)
  - Consistenza dei Processi di Rilevamento (Giallo)
  - Analisi degli Incidenti (Rosso)
  - Miglioramenti al Piano di Ripristino (Verde)
- Metti un marcatore di livello 1 su tutte le seguenti Category:
  - Definizione della Politica Aziendale per la Cybersecurity (Blu)
  - Formazione e Addestramento del Personale (Viola)
  - Sicurezza dei Dati (Viola)
  - Consistenza dei Processi di Rilevamento (Giallo)
  - Contenimento e Mitigazione di un Incidente (Rosso)
  - Gestione delle Comunicazioni in seguito a un Incidente (Verde)
- Metti un marcatore di livello 1 su tutte le seguenti Category:
  - Valutazione del Rischio (Blu)
  - Formazione e Addestramento del Personale (Viola)
  - Manutenzione dei Sistemi Informativi (Viola)
  - Consistenza dei Processi di Rilevamento (Giallo)
  - Contenimento e Mitigazione di un Incidente (Rosso)
  - Gestione delle Comunicazioni in seguito a un Incidente (Verde)

Questo è l'elenco di tutte le carte "Profilo Target" presenti nel gioco:

- Raggiungi il punteggio richiesto per ognuna delle Function:
  - Identificare (Blu) = 7
  - Proteggere (Viola) = 8
  - Rilevare (Giallo) = 3
  - Rispondere (Rosso) = 5

  - Recuperare (Verde) = 2

- Raggiungi il punteggio richiesto per ognuna delle Function:
  - Identificare (Blu) = 6
  - Proteggere (Viola) = 9
  - Rilevare (Giallo) = 3
  - Rispondere (Rosso) = 5
  - Recuperare (Verde) = 2
- Raggiungi il punteggio richiesto per ognuna delle Function:
  - Identificare (Blu) = 5
  - Proteggere (Viola) = 10
  - Rilevare (Giallo) = 4
  - Rispondere (Rosso) = 4
  - Recuperare (Verde) = 2
- Raggiungi il punteggio richiesto per ognuna delle Function:
  - Identificare (Blu) = 6
  - Proteggere (Viola) = 8
  - Rilevare (Giallo) = 4
  - Rispondere (Rosso) = 5
  - Recuperare (Verde) = 2
- Raggiungi il punteggio richiesto per ognuna delle Function:
  - Identificare (Blu) = 6
  - Proteggere (Viola) = 9
  - Rilevare (Giallo) = 4
  - Rispondere (Rosso) = 4
  - Recuperare (Verde) = 2
- Raggiungi il punteggio richiesto per ognuna delle Function:
  - Identificare (Blu) = 6
  - Proteggere (Viola) = 10

  - Rilevare (Giallo) = 3
  - Rispondere (Rosso) = 4
  - Recuperare (Verde) = 2

- Raggiungi il punteggio richiesto per ognuna delle Function:
  - Identificare (Blu) = 6
  - Proteggere (Viola) = 8
  - Rilevare (Giallo) = 3
  - Rispondere (Rosso) = 6
  - Recuperare (Verde) = 2

- Raggiungi il punteggio richiesto per ognuna delle Function:
  - Identificare (Blu) = 7
  - Proteggere (Viola) = 9
  - Rilevare (Giallo) = 3
  - Rispondere (Rosso) = 4
  - Recuperare (Verde) = 2

- Raggiungi il punteggio richiesto per ognuna delle Function:
  - Identificare (Blu) = 5
  - Proteggere (Viola) = 10
  - Rilevare (Giallo) = 3
  - Rispondere (Rosso) = 5
  - Recuperare (Verde) = 2

- Raggiungi il punteggio richiesto per ognuna delle Function:
  - Identificare (Blu) = 5
  - Proteggere (Viola) = 9
  - Rilevare (Giallo) = 3
  - Rispondere (Rosso) = 6
  - Recuperare (Verde) = 2

7.2 Appendice B: Carte "Imprevisto"

Questo è l'elenco di tutte le carte "Imprevisto" presenti nel gioco:

- Il produttore di un software utilizzato dall'azienda rilascia un importante aggiornamento che risolve le vulnerabilità scoperte nell'ultima versione. *Se il livello di maturità del campo "Censimento delle Risorse" è almeno 2, l'inventario delle risorse aziendale sarà aggiornato e si potrà intervenire tempestivamente nell'applicazione dell'aggiornamento nei computer che lo utilizzano. Viceversa, sarà necessario controllare ogni terminale informatico per capire in quali installare l'aggiornamento, perdendo più tempo del necessario (il giocatore perde il suo prossimo turno).*

- Un dipendente dell'azienda deve aggiornare la propria password perchè quella precedente è scaduta. *Se il livello di maturità del campo "Controllo degli Accessi" è almeno 1, la nuova password inserita dall'impiegato viene inviata a un sistema centrale che controlla che rispetti i livelli minimi di sicurezza previsti dall'azienda, se così non è la rifiuta e chiede di inserirne un'altra. Se questo controllo non è presente, il dipendente potrebbe inserire una password poco robusta per gli standard moderni e quindi facilmente violabile, creando una vulnerabilità all'interno dell'azienda. Prendi un segnalino rischio.*

- Un dipendente dell'azienda è preda di un tentativo di phishing e riceve sulla posta elettronica una mail che lo invita ad inserire dati personali riguardanti la sua postazione di lavoro. *Se il livello di maturità del campo "Formazione e Addestramento del personale" è almeno 1, l'impiegato ignora la mail, altrimenti cade nella truffa compromettendo la sicurezza dell'intera azienda. Prendi un segnalino rischio.*

- Per motivi commerciali, è necessario inviare dei dati presenti sui sistemi dell'azienda a un'ente di terze parti. Durante il tragitto, questi dati potrebbero essere intercettati se non sono inviati con metodi crittografici all'avanguardia. *Se il livello di maturità del campo "Sicurezza dei Dati" è almeno 2, i dati sono inviati correttamente utilizzando protocolli moderni e sicuri. Viceversa, alcuni gruppi di malintenzionati potrebbero intercettare informazioni private dell'azienda con la possibilità di causare un danno economico importante a seconda di quali dati sono stati trafugati. Tira un dado da 6, moltiplica il risultato per 10 e paga la somma ottenuta.*

- Si è verificato un guasto all'interno della rete dell'organizzazione, evento che sta rendendo inaccessibili tutte le informazioni e i dati aziendali. *Se il livello di maturità del campo "Configurazione dei Sistemi Informativi" è 2, l'azienda possiede un back-up di tutti i dati a sua disposizione, perciò sarà possibile recuperare quelli salvati in precedenza e metterli a disposizione fintanto che il guasto non sarà risolto. Viceversa, l'azienda non possiede back-up periodici e quindi deve interrompere il proprio servizio fintanto che la situazione normale non viene ripristinata, comportando gravi danni economici all'organizzazione. Paga 30 euro.*

- Solo il personale autorizzato dovrebbe poter gestire e modificare le risorse e i sistemi aziendali, quindi devono essere previsti controlli per evitare che soggetti non autorizzati intervengano in mansioni per le quali non sono preparati. *Se il livello di maturità del campo "Manutenzione dei Sistemi Informativi" è almeno 1, queste procedure di manutenzione vengono effettuate correttamente. Viceversa, senza l'utilizzo di controlli preventivi, alcuni dipendenti non autorizzati potrebbero compiere degli errori e mettere a repentaglio la sicurezza informatica dell'azienda. Questi errori dovono poi essere corretti dal personale addetto, con conseguente perdita di tempo e di risorse (perdi un turno e paga 30 euro)*

- Un attaccante esterno all'organizzazione cerca di connettersi ai sistemi interni della rete aziendale per carpire informazioni riservate. *Se il livello di maturità del campo "Tecnologie Aziendali per la Protezione" è almeno 1, il firewall individua il tentativo di connessione e non ne autorizza il passaggio. Viceversa, l'attaccante riesce ad inserirsi all'interno della rete e può visualizzare dati sensibili dell'organizzazione e installare malware direttamente sui sistemi aziendali. Prendi un segnalino rischio.*

- Un attaccante esterno all'azienda riesce a installare sul server dell'organizzazione uno spyware che monitora tutto il traffico di dati in entrata e in uscita. *Se il livello di maturità del campo "Monitoraggio dei Sistemi Informativi" è almeno 2, lo spyware viene immediatamente isolato e in seguito rimosso dal server. Viceversa, i software di protezione non individuano il malware e l'attaccante può visionare le informazioni riservate dell'azienda e in seguito pianificare un ulteriore attacco. Prendi un segnalino rischio.*

- *Se il livello di maturità del campo "Contenimento e Mitigazione di un Incidente" è inferiore a 2, le misure di sicurezza non sono state in grado di limitare un incidente interno all'organizzazione. Subisci immediatamente un attacco informatico (questa carta conta come un segnalino rischio nel calcolo dei danni).*

- Si è verificato un incidente all'interno dell'azienda che però è stato contenuto efficacemente dai meccanismi di risposta. È necessario ora ripristinare la situazione precedente al verificarsi dell'incidente. *Se il livello di maturità del campo "Piano di Ripristino" è 1, sono eseguite le procedure per assicurare un tempestivo recupero dei sistemi. Viceversa, i ritardi causati dal ritorno all'operatività normale si traducono in danni economici per l'azienda. Paga 30 euro.*

- Un gruppo di hacker effettua un tentativo di attacco informatico contro l'azienda. *Il giocatore subisce un attacco informatico e questa carta conta come se fosse un segnalino rischio.*

- Il consiglio di amministrazione è stato rinviato. *Gioca un altro turno ma muoviti all'indietro sul tabellone.*

7.3 Appendice C: Carte "Probabilità"

Questo è l'elenco di tutte le carte "Probabilità" presenti nel gioco:

- Utilizzando un inventario delle risorse è possibile identificare i sistemi con maggiore rilevanza per il conseguimento degli obiettivi aziendali. Nel caso di un incidente, è così possibile intervenire tempestivamente su questi sistemi in maniera prioritaria. *Se il livello di maturità del campo "Censimento delle Risorse" è almeno 1, tieni da conto questa carta per utilizzarla nel caso di un attacco informatico e prevenire una parte dei danni previsti dall'incidente (questa carta vale 30 euro per pagare i danni causati da un attacco informatico).*

- Se all'interno di un'organizzazione viene identificata una figura che rappresenti il punto di riferimento per la sicurezza informatica, è possibile ottenere un'efficace operatività, intesa come attuazione dei controlli di prevenzione e contrasto delle minacce di cybersecurity. *Se il livello di maturità del campo "Definizione della Politica Aziendale per la Cybersecurity" è almeno 1, scegli un campo Viola o Giallo e aumenta il suo livello di maturità pagando il costo necessario (questa azione è facoltativa).*

- *Se il livello di maturità del campo "Valutazione del Rischio" è almeno a 1, tieni da conto questa carta e usala in qualsiasi momento per aumentare di 1 il livello di maturità di un campo qualsiasi per la durata di un turno (non conta per la vittoria finale).*

- All'interno dell'organizzazione solo gli utenti effettivamente autorizzati dovrebbero poter accedere ai sistemi aziendali e alle informazioni presenti in essi, assegnando inoltre ad ogni dipendente le credenziali di accesso con i privilegi minimi necessari a esercitare le mansioni relative. *Se il livello di maturità del campo "Controllo degli Accessi" è 3, allora la segregazione dei ruoli viene applicata in modo tale che ogni sistema sensibile non possa venire modificato da chi non ha i privilegi per accederci, rendendo l'intera rete aziendale più sicura da errori interni. Puoi quindi alzare di uno il livello di maturità di una qualsiasi Category della Function "Proteggere" senza pagare i costi necessari.*

- Gli utenti delle aziende che interagiscono con i sistemi informatici rappresentano la principale fonte di rischio: i comportamenti non consoni o errati possono vanificare le più sofisticate misure di sicurezza adottate dall'azienda. *Se il livello di maturità del campo*

"Formazione e Addestramento del Personale" è almeno 2, gli utenti lavorano in completa sicurezza e hanno la conoscenza necessaria per gestire immediatamente anomalie che si possono verificare durante l'utilizzo dei sistemi informatici dell'organizzazione. Con queste capacità i dipendenti sono più efficienti e l'azienda ha una probabilità maggiore di raggiungere i suoi obiettivi. Guadagna 40 euro.

- I computer e i dispositivi di rete non possono essere considerati sicuri quando configurati con le impostazioni standard fornite in origine dai produttori. *Se il livello di maturità del campo "Configurazione dei Sistemi Informativi" è almeno 1, tutti i nuovi sistemi vengono configurati appropriatamente, disabilitando le utenze non strettamente necessarie, cambiando qualsiasi password pre-impostata e rimuovendo/disabilitando i software e i servizi non necessari. Questo rende i sistemi informativi dell'azienda più sicuri nel loro complesso. Tieni da conto questa carta e utilizzala per dimezzare i costi di ampliamento di una qualsiasi Category.*

- Viene effettuata una scansione dei sistemi informativi alla ricerca di possibili vulnerabilità. *Il giocatore tira il dado una volta: se il livello del campo "Monitoraggio Periodico dei Sistemi Informativi" è 1 e il risultato del lancio è almeno un 5, è possibile scartare un segnalino rischio; se il livello di questo campo è 2 e il risultato del lancio è almeno un 3, è possibile scartare un segnalino rischio; se il livello di questo campo è 3 e il risultato del lancio non è 1, è possibile scartare un segnalino rischio.*

- *Se il livello di maturità del campo "Rilevamento delle Anomalie" è almeno 2, i sensori avvisano i responsabili di un'attività anomala nei sistemi dell'azienda ed è quindi possibile gestirla per tempo. Scarta un segnalino rischio (se ne hai).*

- Per proteggere l'azienda da incidenti di sicurezza, è necessario lavorare sulla prevenzione, analizzare gli incidenti passati e limitare la possibilità di occorrenze future. *Se il livello di maturità del campo "Contenimento e Mitigazione di un Incidente" è almeno 2, tieni da conto questa carta per prevenire il prossimo attacco informatico (se ottieni il terzo segnalino rischio, scartalo).*

- *Se il livello di maturità dei campi "Analisi degli Incidenti" e "Rilevamento delle Anomalie" è almeno 1 in entrambi, l'organizzazione è preparata a rispondere ad un possibile evento di*

sicurezza avverso. Tieni da conto questa carta e, durante un attacco informatico, usala per scartare immediatamente un segnalino rischio.

- I vertici aziendali hanno dato il permesso per organizzare una riunione con il personale per giocare a Securopoly. *Vai alla casella "Formazione e Addestramento del personale" oppure ignora questa carta.*

- Ultimamente l'azienda di cui fai parte sta riscuotendo un notevole successo, tanto che le sue azioni hanno influenze sul mercato e sulle altre organizzazioni. *Se c'è una carta "Mercato" attiva, puoi scegliere di lasciarla al suo posto oppure scartarla; se la scarti, puoi scegliere di pescare un'altra carta "Mercato" da rendere immediatamente attiva. Se non è presente nessuna carta "Mercato" attiva puoi decidere di pescarne una.*

7.4 Appendice D: Carte "Mercato"

Questo è l'elenco di tutte le carte "Mercato" presenti nel gioco:

- Il governo ha emanato agevolazioni e incentivi per le aziende che investono nella cybersecurity. *I costi necessari ad aumentare il livello di maturità di una qualsiasi Category sono dimezzati.*
- È un periodo di crisi economica e l'azienda ha dovuto tagliare il budget a disposizione di alcuni suoi reparti, compreso quello per la cybersecurity. *Il Consiglio di Amministrazione elargisce la metà della somma normale.*
- La fortuna aiuta gli audaci... *Tutte le caselle "Imprevisto" diventano caselle "Probabilità".*
- Gli imprevisti sono sempre dietro l'angolo... *Tutte le caselle "Probabilità" diventano caselle "Imprevisto".*
- All'interno di un software molto diffuso tra le aziende, è presente un bug non ancora noto pubblicamente. Fintanto che questa vulnerabilità non viene risolta, è possibile incorrere in uno 0-day attack, ovvero un attacco che sfrutta un bug di un software che non è stato ancora risolto dal produttore. *Ogni giocatore prende un segnalino rischio. Dopo che ogni giocatore ha completato questa azione, scarta questa carta. Se un giocatore ha ottenuto in questo modo il suo terzo segnalino, subisce un attacco informatico con le stesse modalità come se fosse il suo turno.*
- Le leggi del mercato sono imprevedibili... *Fintanto che questa carta è attiva, i giocatori si muovono in senso antiorario lungo il tabellone; inoltre anche i turni dei giocatori sono invertiti, quindi il gioco passa alla persona alla destra dell'ultimo giocatore che ha tirato. Quando questa carta viene scartata viene ripristinato il senso orario.*
- *Dopo aver tirato il dado la prima volta per muoversi a inizio turno, il giocatore può decidere se accettare tale risultato o ritirare nuovamente il dado.*
- Sono state aggiornate le linee guida e le tecniche da tenere per la difesa contro la cybersecurity all'interno del Framework Nazionale, per questo motivo è necessario aggiornare la strategia aziendale di conseguenza alle nuove norme. *Tutti i giocatori tornano alla casella*

"Consiglio di Amministrazione" e ricevono la metà dei fondi previsti dal passaggio su tale casella. Scarta questa carta.

- *Uno alla volta, ogni giocatore tira il dado: se il risultato è 1, non succede niente; se il risultato è 2, il giocatore muove la sua pedina su un campo Blu a sua scelta; se il risultato è 3, il giocatore muove la sua pedina su un campo Viola a sua scelta; se il risultato è 4, il giocatore muove la sua pedina su un campo Giallo a sua scelta; se il risultato è 5, il giocatore muove la sua pedina su un campo Rosso a sua scelta; se il risultato è 6, il giocatore muove la sua pedina su un campo Verde a sua scelta. Inoltre, i giocatori possono decidere se aumentare il livello di maturità del campo su cui si muovono pagando il relativo costo. Alla fine di questo processo, scarta questa carta.*

- Ad ogni giocatore vengono assegnati dei bonus dalla loro organizzazione per i risultati ottenuti fino a questo momento. *I giocatori contano la somma dei livelli di maturità di tutte le Category, il risultato moltiplicato per 2 (approssimato al numero più vicino divisibile per 5) è l'entità del bonus che gli viene assegnato.*

7.5 Appendice E: Elenco dei livelli di maturità per ogni Category

Questo è l'elenco di tutti i livelli di maturità che caratterizzano tutte le Category presenti lungo il tabellone.
Le seguenti sono le Category appartenenti alla Function "Identificare":

- **Censimento delle Risorse**:
  1) I sistemi informatici sono classificati manualmente
  2) I sistemi informatici sono registrati automaticamente ma il loro aggiornamento avviene in modo manuale
  3) I sistemi informatici sono classificati e aggiornati automaticamente

- **Definizione degli Obiettivi**:
  1) Ad ogni attività dell'organizzazione vengono assegnate delle prioritè che individuano quanto tale operazione è importante per l'azienda

- **Definizione della Politica Aziendale per la Cybersecurity**:
  1) Viene nominato un referente per la sicurezza informatica e vengono definite le attività di cui è responsabile
  2) Viene predisposto formalmente un documento che definisce i ruoli e le à di ciascuna parte coinvolta nella gestione della sicurezza informatica

- **Valutazione del Rischio**:
  1) Le vulnerabilità dell'organizzazione vengono identificate
  2) Le vulnerabilità dell'organizzazione vengono identificate, documentate e ad ognuna di esse viene assegnata una probabilità di accadimento

- **Strategia per la gestione del rischio**:
  1) Il rischio tollerato dall'organizzazione è calcolato ed espresso chiaramente

Le seguenti sono le Category appartenenti alla Function "Proteggere":

- **Controllo degli Accessi**:
  1) Le credenziali di accesso alle risorse sono amministrate attraverso una directory aziendale che consente l'applicazione omogenea di regole e livelli minimi di sicurezza
  2) L'accesso remoto alle risorse avviene attraverso l'uso di canali di comunicazione sicuri
  3) Gli accessi alle risorse vengono concessi coerentemente alle funzioni previste da ciascun ruolo, al fine di prevenire o identificare la possibilità di frodi, abusi o errori da parte degli utenti

- **Formazione e Addestramento del Personale**:
  1) La formazione di base del personale sui rischi di cybersecurity avviene attraverso l'ausilio di strumenti appropriati e secondo una pianificazione ed una periodicità definite
  2) Le iniziative di formazione sulla cybersecurity vengono differenziate nei loro obiettivi e nei contenuti in base allo specifico ruolo svolto dal personale coinvolto
  3) La formazione del personale specifico sulla cybersecurity viene svolta mediante il supporto di organizzazioni esterne prevedendo eventuali percorsi di certificazione professionale

- **Sicurezza dei Dati**:
  1) I dati e le informazioni memorizzate all'interno dell'organizzazione sono protette
  2) I sistemi hanno adeguate risorse a disposizione per garantire l'integrità, la confidenzialità e la disponibilità dei dati e delle informazioni

- **Configurazione dei Sistemi Informativi**:
  1) La configurazione sicura dei sistemi avviene attraverso il ricorso a linee guida e procedure operative secondo gli standard di mercato
  2) Viene configurato e verificato periodicamente il back-up dei dati aziendali, il quale avviene mediante soluzioni tecnologiche specifiche

- **Manutenzione dei Sistemi Informativi**:

1) La manutenzione e la riparazione delle risorse e dei sistemi è registrata e svolta attraverso l'utilizzo di strumenti controllati ed autorizzati
2) La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati

- **Tecnologie Aziendali per la Protezione**:

1) Le reti di comunicazione interne all'azienda sono protette da un firewall che limita il traffico a solo quello autorizzato
2) L'accesso alle risorse e ai sistemi è limitato secondo il principio di minima funzionalità

Le seguenti sono le Category appartenenti alla Function "Rilevare":

- **Rilevamento delle Anomalie**:

1) Vengono determinati gli impatti di possibili eventi anomali
2) Vengono definite soglie di allerta e vengono usati sensori e sorgenti multiple per rilevare tempestivamente attività anomale

- **Monitoraggio dei Sistemi Informativi**:

1) Il codice malevolo viene rilevato tramite soluzioni tecnologiche dedicate
2) Il personale, le connessioni, i dispositivi e il software non autorizzato vengono rilevati
3) Il sistema di rilevamento anomalie è gestito a livello centrale e vengono combinate assieme soluzioni tecnologiche diverse

- **Consistenza dei Processi di Rilevamento**:

1) I processi di monitoraggio vengono testati e sono oggetto di periodici miglioramenti

Le seguenti sono le Category appartenenti alla Function "Rispondere":

- **Piano di Risposta ad un Incidente**:

1) Sono definite le procedure di risposta da eseguire durante un incidente

- **Analisi degli Incidenti**:
  1) Le notifiche provenienti dai sistemi di monitoraggio vengono visionate e analizzate per assicurare un'adeguata risposta
  2) L'impatto di ogni incidente viene compreso e viene svolta un'analisi forense
- **Coordinamento delle Operazioni di Risposta**:
  1) Le informazioni sono condivise con le parti interne ed esterne all'organizzazione per ottenere supporto e una maggiore consapevolezza della situazione
- **Contenimento e Mitigazione di un Incidente**:
  1) In caso di incidente vengono messe in atto procedure atte a prevenirne l'espansione e a mitigarne gli effetti
  2) Gli incidenti e le attività completate per la loro gestione sono registrate per determinare le cause e ridurre la probabilità di accadimento
  3) Le vulnerabilità conosciute sono mitigate o documentate come rischio accettato
- **Miglioramenti al Piano di Risposta**:
  1) Le procedure di risposta sono migliorate tenendo conto delle esperienze passate

Le seguenti sono le Category appartenenti alla Function "Recuperare":

- **Piano di Ripristino**:
  1) Sono definite le procedure di ripristino dei sistemi coinvolti in seguito ad un incidente
- **Miglioramenti al Piano di Ripristino**:
  1) Le procedure di ripristino sono migliorate tenendo conto delle esperienze passate
- **Gestione delle Comunicazioni in seguito ad un Incidente**:
  1) In seguito ad un incidente sono gestite le pubbliche relazioni e viene ripristinata la reputazione

BIBLIOGRAFIA

[1] Mackenzie Adams e Maged Makramalla. "Cybersecurity Skills Training: An Attacker-Centric Gamified Approach". In: *Technology Innovation Management Review* 5.1 (2015).

[2] Roberto Baldoni e Luca Montanari. *Un Framework Nazionale per la Cyber Security*. Ver. 1.0. 2016. URL: `http://www.cybersecurityframework.it`.

[3] K. Boopathi, S. Sreejith e A. Bithin. "Learning cyber security through gamification". In: *Indian Journal of Science and Technology* 8.7 (2015), pp. 642–649.

[4] Benjamin D. Cone et al. "A video game for cyber security training and awareness". In: *Computers & Security* 26.1 (2007), pp. 63–72.

[5] Ian Cullinane et al. "Cyber security education through gaming: cybersecurity games can be interactive, fun, educational and engaging". In: *Journal of Computing Sciences in Colleges* 30.6 (2015), pp. 75–81.

[6] Sandro Fouché e Andrew H. Mangle. "Code hunt as platform for gamification of cybersecurity training". In: *Proceedings of the 1st International Workshop on Code Hunt Workshop on Educational Software Engineering*. ACM. 2015, pp. 9–11.

[7] Christopher Herr e Dennis Allen. "Video Games as a Training Tool to Prepare the Next Generation of Cyber Warriors". In: *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*. ACM. 2015, pp. 23–29.

[8] Cara McGoogan. "Want to be a GCHQ spy? Play this game". In: *Wired.uk* (ott. 2015). URL: `http://www.wired.co.uk/article/cyphinx-cybersecurity-game`.

[9] Antoine M. Melki e Moussa G. Chatrieh. *Gamification to Support Cyber Security Community Education in Lebanon*. URL: `http://docplayer.net/2657177-Gamification-to-support-cyber-security-community-education-in-lebanon.html`.