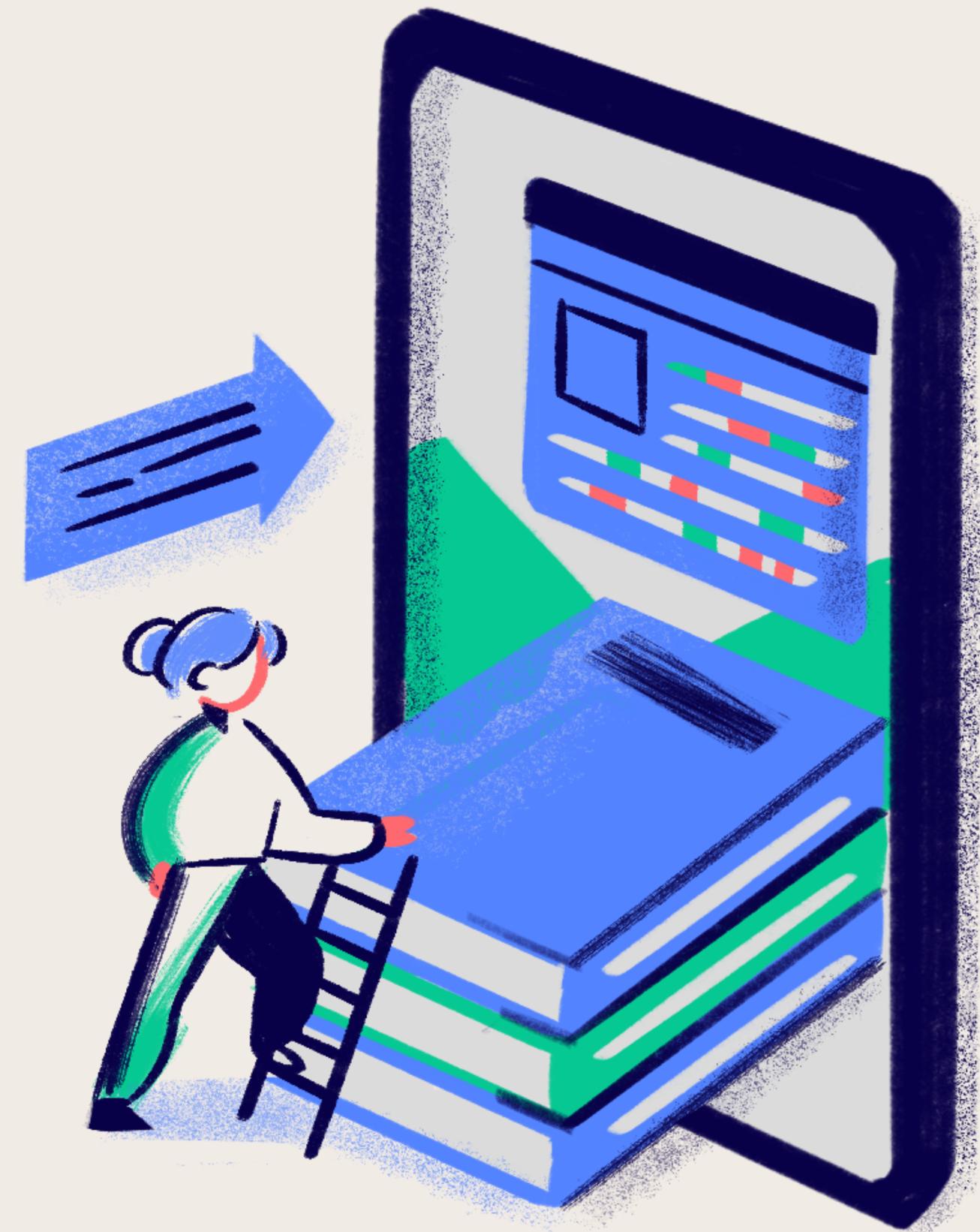


PROGETTO S1/L5

RISK ASSESSMENT



MATTIA CHIRIATTI
MARCO D'ANTONI



TRACCIA

La vostra organizzazione vi ha incaricato di svolgere un risk assessment sulla seguente azienda.

Nome azienda: TechnoCorp

Settore: Tecnologia dell'informazione e servizi IT

Descrizione: TechnoCorp è un'azienda di medie dimensioni che opera nel settore IT, fornendo servizi di consulenza, sviluppo software e gestione di infrastrutture tecnologiche a clienti di diverse industrie.

Fondata 15 anni fa, l'azienda conta circa 500 dipendenti distribuiti tra la sede centrale e 3 filiali regionali. Infrastruttura IT:

- Rete aziendale con server interni che ospitano applicazioni aziendali critiche, database e sistemi di archiviazione dati
- Utilizzo di cloud pubblici (AWS, Azure) per alcune applicazioni e servizi
- Rete wireless per dipendenti e guest
- Dispositivi personali (Bring Your Own Device) utilizzati dai dipendenti
- Numerosi laptop e workstation per sviluppatori e consulenti
- Sito web aziendale ospitato esternamente
- Firewall Perimetrale
- EDR/xDR su tutti i sistemi



TRACCIA

Clienti e dati sensibili

- TechnoCorp gestisce dati sensibili di clienti, come informazioni finanziarie, dati personali di dipendenti/clienti, proprietà intellettuale;
- I principali clienti includono banche, assicurazioni, aziende sanitarie e produttori

Personale e accessi:

- Amministratori di sistema con accesso totale all'infrastruttura;
- Sviluppatori con accesso ai sistemi di sviluppo;
- Personale di supporto tecnico con accesso limitato;
- Consulenti e collaboratori esterni con credenziali di accesso;
- Politica di password e autenticazione a due fattori implementata

Partendo dalla descrizione fornita, procedere con l'identificazione di uno scenario di rischio (Top-down) fino ad arrivare all'analisi del rischio di questo scenario.

- Identificazione del rischio
- Analisi degli asset
- Analisi delle vulnerabilità
- Analisi delle minacce
- Modellazione delle minacce
- Scenari di rischio
- Analisi del rischio qualitativa o semi-quantitativa

Per le probabilità di occorrenza, statistiche e stime, affidatevi a fonti note o studi di settore.

RISK IDENTIFICATION

Dopo una breve analisi, abbiamo individuato due rischi che coprono diverse categorie di rischi a livello organizzativo/aziendale, ovvero il rischio legato ai dispositivi BYOD e il rischio legato alla rete Wi-Fi condivisa fra dipendenti e guest.

I dispositivi BYOD implicano un rischio legato a infezioni da malware provenienti da reti esterne a quelle aziendali: non è insolito infatti per un malware scansionare l'intera rete a caccia di dispositivi o risorse vulnerabili, su cui installare eseguibili malevoli per prenderne il controllo.

In aggiunta, un dipendente potrebbe tramutarsi in una minaccia Insider, mettendo a repentaglio l'integrità e, più in generale, l'intera sicurezza dei dati sensibili aziendali.

Una rete Wi-Fi condivisa e non segmentata potrebbe essere facilmente vittima di un hacker, in quanto poco sicura e di quasi libero accesso nonostante il riconoscimento a due fattori o l'utilizzo di credenziali di accesso.

Le minacce, come anticipato, coprono diverse categorie di rischio:



ANALISI DEGLI ASSET

Asset	Quantità	Valore Unitario	Valore Totale
Dipendenti	500	1.000.000,00 €	500.000.000,00 €
Laptop (Lenovo ThinkPad X1 Carbon Gen 12)	250	1.999,00 €	499.750,00 €
Workstation (HP Z2 Tower G9)	250	1.999,00 €	499.750,00 €
Sito Aziendale Esterno	1	6000€/Mese	
Cloud (Awe, Azure)	1	100€/Mese	
Database (Storage Super Server 640SP-E1CR60)	10	16.000,00 €	160.000,00 €
XDR (Sophos Intercept X)	600	48,00 €	28.800,00 €
Firewall Perimetrale (Fortinet FORTIGATE-6300F)	1	300.000,00 €	300.000,00 €
Server (Hewlett Packard Enterprise Hpe ProLiant ML350 Gen10)	50	3.000,00 €	150.000,00 €
Router Wireless (D-Link DSR-1000AC)	50	500,00 €	25.000,00 €

- Sito Aziendale Esterno: il valore unitario di questo asset comprende tutti i costi di manutenzione, gestione e cura dei dati sensibili all'interno del suo database;
- Nella voce Server vanno considerati tutti i server descritti nella traccia;
- L'alto numero di router è collegato all'alto numero di dispositivi che dovranno andare a gestire, fra quelli interni all'azienda e i dispositivi personali dei dipendenti.

ANALISI DELLE MINACCIE

Minaccia	Descrizione	Vettore di Attacco	Fonte di Minaccia	Probabilità (Prima)	Controllo di Mitigazione	Costo Mitigazione	Probabilità (Dopo)
Ingegneria Sociale	Accesso non autorizzato alla rete	Email di Phishing	Hacker	Alta	Formazione sulla sicurezza informatica, software anti phishing	Medio	Bassa
Accesso non autorizzato	Hacking dei sistemi tramite sfruttamento di vulnerabilità	Rete, applicazioni web	Hacker, Insider	Media	VPN, segmentazione della rete	Medio	Bassa
Errore umano	Configurazioni errate, violazioni di policy di sicurezza	Azioni degli utenti interni	Dipendenti	Alta	Formazione sulla sicurezza informatica, policy di sicurezza chiare e definite	Basso	Media
Malware Ransomware	Cripta i dati dell'organizzazione con richiesta di riscatto	Email di Phishing, siti web malevoli	Hacker	Alta	Formazione sulla sicurezza informatica, software antivirus/antimalware, backup regolari	Medio	Bassa
Incendio	Distruzione di server	Mancato controllo delle temperature nelle server room	Ambiente	Media	Sistema di climatizzazione automatico	Medio	Bassa
BYOD Intrusion	Attacco malware tramite infiltrazione su BYOD	Dispositivi BYOD	Hacker, Insider	Alta	Limitazione degli accessi dei dispositivi BYOD, eliminazione dei dispositivi BYOD	Alto	Bassa

ANALISI DELLE VULNERABILITÀ

Principali Vulnerabilità

Server

- CVE-2024-23897: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-23897>
- Jenkins 2.441 e versioni precedenti, LTS 2.426.2 e versioni precedenti non disabilitano una funzionalità del parser dei comandi CLI che sostituisce un carattere "@" seguito da un percorso di file in un argomento con il contenuto del file, consentendo agli aggressori non autenticati di leggere file arbitrari sul File system del controller Jenkins.
- CVE-2017-9841: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9841>
- Util/PHP/eval-stdin.php in PHPUnit prima della 4.8.28 e 5.x prima della 5.6.3 consente agli aggressori remoti di eseguire codice PHP arbitrario tramite dati HTTP POST che iniziano con una sottostringa "<?php ", come dimostrato da un attacco su un sito con una cartella /vendor esposta, ovvero accesso esterno all'URI /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php.
- CVE-2021-3129: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3129>
- Ignition prima della versione 2.5.2, utilizzata in Laravel e altri prodotti, consente agli aggressori remoti non autenticati di eseguire codice arbitrario a causa dell'utilizzo non sicuro di file_get_contents() e file_put_contents(). Questo è sfruttabile sui siti che utilizzano la modalità debug con Laravel prima della 8.4.2.

ANALISI DELLE VULNERABILITÀ

- CVE-2021-28481: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28481>
- Vulnerabilità legata all'esecuzione di codice in modalità remota di Microsoft Exchange Server

- CVE-2021-26086: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26086>
- Le versioni interessate di Atlassian Jira Server e Data Center consentono agli aggressori remoti di leggere determinati file tramite una vulnerabilità di attraversamento del percorso nell'endpoint /WEB-INF/web.xml. Le versioni interessate sono precedenti alla versione 8.5.14, dalla versione 8.6.0 prima della 8.13.6 e dalla versione 8.14.0 prima della 8.16.1.

Interazione con componenti esterni

- Policy di sicurezza assenti per il BYOD troppo permissivo
- Segmentazione assente fra la rete Wifi Interna ed Esterna

THREAT MODELING - BYOD

Per iniziare un'analisi del rischio di tipo top-down, ci avvaliamo del framework di Shostack, utilizzando le sue 4 domande per delineare la minaccia individuata nella fase preliminare, ovvero una minaccia legata ai dispositivi BYOD.

1. What are we working on? → Sviluppo software e gestione infrastrutture tecnologiche

2.What can go wrong? → Dispositivi BYOD infetti, furto di dati sensibili

3.What are we going to do about it? → Eliminazione dispositivi BYOD, limitazioni all'accesso ai dati

4.Did we do a good job? → Controllo costante sul rispetto della policy BYOD, monitoraggio costante delle limitazioni all'accesso ai dati

THREAT MODELING - RETE WIFI

Per iniziare un'analisi del rischio di tipo top-down, ci avvaliamo del framework di Shostack, utilizzando le sue 4 domande per delineare la minaccia individuata nella fase preliminare, ovvero una minaccia legata alla rete Wi-Fi.

1. What are we working on? → Sviluppo software e gestione infrastrutture tecnologiche

2.What can go wrong? → Un criminale Informatico potrebbe accedere alla rete interna tramite la rete Wi-Fi condivisa e non segmentata

3.What are we going to do about it? → Segmentazione della rete

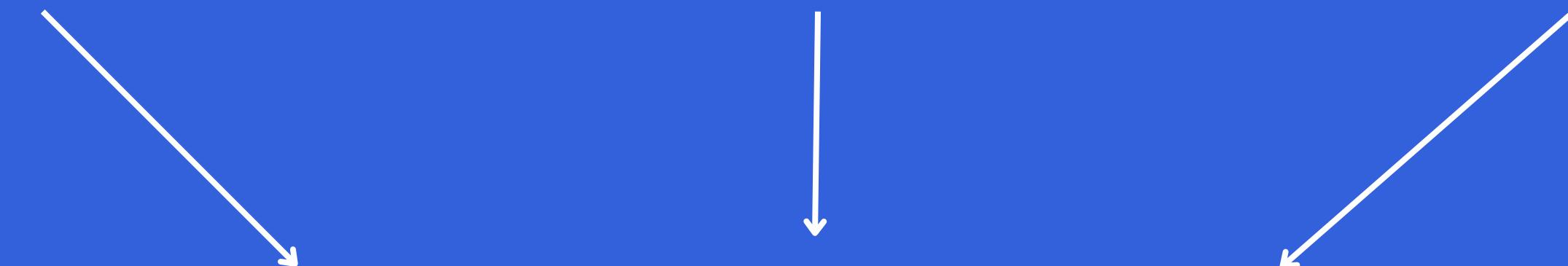
4.Did we do a good job? → Testare la nuova rete per assicurare una corretta segmentazione

RISK SCENARIO

DISPOSITIVI BYOD

MALWARE, INSIDERS

RETE INTERNA, DATI SENSIBILI



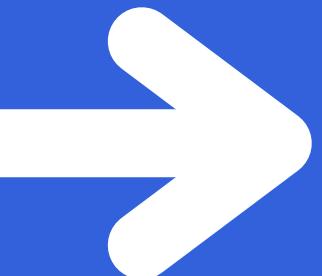
**BYOD INTRUSION/ ATTACCO ALLA
RETE INTERNA**

RISK SCENARIO - GAP ANALYSIS

GAP - BYOD

Stato Corrente

Scarsa protezione contro possibili attacchi provenienti da dispositivi BYOD



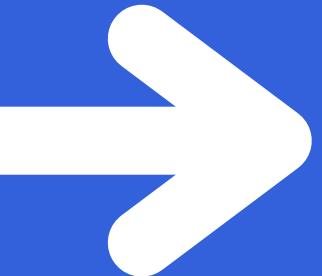
Stato desiderato

Eliminazione dei dispositivi BYOD e susseguente miglioramento della protezione aziendale

GAP - WIFI

Stato Corrente

Rete non segmentata e, quindi, non sicura in quanto condivisa fra i dipendenti e guest



Stato desiderato

Rete segmentata e sicura

RISK SCENARIO - GAP ANALYSIS

ACTION PLAN - BYOD

- **Delineare una nuova policy per eliminare i dispositivi BYOD**
- **Informare i dipendenti sulle ragioni di questa scelta strategica aziendale**
- **Valutazione sui possibili dispositivi da acquistare**
- **Acquisto dei dispositivi**
- **Implementazione sistemi di sicurezza nei dispositivi**
- **Integrazione con riconoscimento a 2 fattori, come da compliance aziendale**
- **Integrazione di un sistema di monitoraggio degli accessi**

RISK SCENARIO - GAP ANALYSIS

ACTION PLAN - RETE WIFI

- **Analisi della rete: individuazione del numero di sottoreti da creare**
- **Segmentazione della rete**
- **Messa in sicurezza della rete**
- **Testing della segmentazione**

RISK SCENARIO - GAP ANALYSIS

ROADMAP - BYOD



RISK SCENARIO - GAP ANALYSIS

ROADMAP - RETE WIFI



ANALISI SEMI-QUANTITATIVA

*Single Loss Expectancy o Asset Value per incidente = €500.000**

Annual Rate of Occurrence = 10

*Annual Loss Expectancy = SLE * ARO = €5.000.000*

Fatturato annuo = €10.400.000

Impatto = ALE/Fatturato = 5.000.000/10.400.000 = 48.1%

Verosomiglianza = 75%

ANALISI SEMI-QUANTITATIVA

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	If the threat is initiated or occurs, it is almost certain to have adverse impacts
High	80-95	8	If the threat is initiated or occurs, it is highly likely to have adverse impacts
Moderate	21-79	5	If the threat is initiated or occurs, it is somewhat likely to have adverse impacts
Low	5-20	2	If the threat is initiated or occurs, it is unlikely to have adverse impacts
Very Low	0-4	0	If the threat is initiated or occurs, it is highly unlikely to have adverse impacts

Basando la nostra analisi sulla NIST SP 800-30 Rev.1, Guide for Conducting Risk Assessment, Table G-4: Assessment Scale - Likelihood of Threat Event Resulting in Adverse Impacts, la probabilità legata all'evento avverso sull'azienda è Moderate, in quanto il suo tasso di Verosimiglianza è pari al 75%.

ANALISI SEMI-QUANTITATIVA

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	The threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries
Moderate	21-79	5	The threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low	5-20	2	The threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	0-4	0	The threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

Basando la nostra analisi sulla NIST SP 800-30 Rev.1, Guide for Conducting Risk Assessment, Table H-3: Assessment Scale - Impact of Threat Events, l'impatto dell'evento avverso sull'azienda è Moderate, in quanto il suo tasso di Impatto è pari allo 48.1%.

ANALISI SEMI-QUANTITATIVA

Likelihood (Threat Event Occurs and results in Adverse Impact)	Level Of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Basando la nostra analisi sulla NIST SP 800-30 Rev.1, Guide for Conducting Risk Assessment, Table I-2: Assessment Scale - Level of Risk (Combination of Likelihood and Impact), il livello di rischio dell'evento avverso sull'azienda è Moderato, in quanto prodotto della combinazione di una Verosomiglianza di un Impatto Moderati.

**THANK
YOU VERY
MUCH!**

