TABELLA I-5: RISCHIO CONTROVERSO												
1	2	3	4	5	6	7	8	9	10	11	12	13
Treat event	Threat source	Threat source Characteristics			Relevance	Likleihood of attack initiation	Vulnerabilities and predisposing conditions	Likelihood Initialited Attack Successeds	Severity and pervasiveness	Overall likelihood (G-5)	Level of Impact	Risk (I-2)
		Capability	Intent	Targeting								
L'avversario adatta il comportamento in risposta alla sorveglianza e alle misure di sicurezza organizzative.	Un attaccante compromette la sicurezza dei server aziendali attraverso vulnerabilità software o tecniche di phishing	Alto	Medio	Alto	Confermato	Alto	Informazioni di identificazione personale: Ha bisogno di utilizzare le tecnologie in modi specifici.	Alto	Molto alto	Alto	Alto	Medio
L'avversario intraprende azioni per inibire l'efficacia dei sistemi di rilevamento delle intrusioni o delle capacità di controllo all'interno delle organizzazioni.		Alto	Medio	Alto	Previsto	Medio	Ha bisogno di utilizzare le tecnologie in modi specifici.	Alto	Molto alto	Alto	Alto	Medio
L'avversario adatta il comportamento in risposta alla sorveglianza e alle misure di sicurezza organizzative.		Alto	Medio	Alto	Previsto	Medio	Programmi di accesso speciale	Alto	Molto alto	Alto	Alto	Medio
L'avversario scansiona o estrae informazioni su server e pagine Web di organizzazioni accessibili pubblicamente con l'intento di trovare informazioni sensibili.	Un attaccante compromette la sicurezza dei server aziendali attraverso vulnerabilità software o tecniche di phishing	Alto	Medio	Alto	Confermato	Molto alto	Determinato dall'accordo con il gestore del cloud	Alto	Molto alto	Alto	Alto	Medio

TABELLA I-5: RISCHIO CONTROVERSO												
1	2	3	4	5	6	7	8	9	10	11	12	13
Treat event	Threat source	Threat source Characteristics			Relevance	Likleihood of attack initiation	Vulnerabilities and predisposing conditions	Likelihood Initialited Attack Successeds	Severity and pervasiveness	Overall likelihood (G-5)	Level of Impact	Risk (I-2)
		Capability	Intent	Targeting								
L'avversario contamina i sistemi informativi organizzativi (inclusi dispositivi e reti) inducendoli a gestire informazioni di una classificazione/sensibilità per la quale non sono stati autorizzati. Le informazioni vengono esposte a individui non autorizzati ad accedervi e il sistema informativo, il dispositivo o la rete non sono disponibili mentre la fuoriuscita viene indagata e mitigata.	Un attaccante compromette la sicurezza dei server aziendali attraverso vulnerabilità software o tecniche di phishing	Alto	Medio	Alto	Possibile	Medio	Informazioni di identificazione personale	Alto	Molto alto	Alto	Alto	Medio
I dipendenti dell'azienda potrebbero rappresentare una minaccia interna se agiscono in modo malevolo o se commettono errori non intenzionali	La divulgazione non autorizzata di informazioni sensibili	Alto	Medio	Medio	Possibile	Basso	Errore umano nel aprire link malevoli	Alto	Molto alto	Alto	Alto	Medio