信息與管理 58 (2021) 103318

內容列表可在科學指導

信息與管理

期刊主頁：www.elsevier.com/locate/im

多級制裁對信息安全政策合規性影響的威懾作用：多組分析的結果

倫納特耶格A,*, 安德烈亞斯・埃克哈特b,C, 朱莉婭・克羅農A

A*EBS 商業與法律大學，管理與經濟系，Rheingaustraße 1, 65375, Oestrich-Winkel, 德國*
b*德國管理與法律研究生院，Bildungscampus 2, 74076, Heilbronn, Germany*
C*因斯布魯克大學，商業與管理學院，Universitaetsstraße 15, 6020, 因斯布魯克, 奧地利*

文章信息

關鍵詞：
信息安全政策合規態度

威懾
制裁
威懾力
信息安全政策意識

抽象的

本文提供了製裁影響信息安全政策合規性有效性的新視角。我們從群體的角度觀察合規性，以識別基於內心信念而遵守的不可威懾員工和因外部脅迫而遵守的可威懾員工。根據調查數據，我們表明多層次製裁（即正式、社會和個人制裁）對傾向於和不傾向於的員工的合規性有不同的影響。我們還發現，多級制裁感知受信息安全政策意識的不同影響。這種基於群體的威懾性觀點開闢了研究制裁價值的新途徑。

一、簡介

雖然外部因素（如黑客和惡意軟件）對組織的信息安全構成相當大的威脅，但員工的行為通常被認為具有更高的安全風險[1個]. 減少與此類員工相關的信息安全威脅的一個關鍵工具是創建、部署和執行信息安全策略。這些政策規定了員工在正確使用和保護組織信息系統 (IS) 資源方面的角色和責任 [2個,3個]. 然而，據廣泛報導，許多員工不遵守這些政策或故意繞過這些政策[4個]. 雖然員工通常不想傷害他們的組織，但在大多數情況下，他們沒有足夠的動力去遵守政策 [4個]. 具體而言，在當今數字驅動的世界中，速度、生產力和適應性正在推動和定義員工的能力，使其更快、更高效，員工行為的特徵通常是訪問或使用未事先獲得信息技術部門批准的外部系統（IT部門 [5個]. 一個這樣的例子是公共雲系統，例如 Dropbox，許多員工使用它來保存和共享公司數據，而不考慮組織信息安全策略 [5個]. 甲骨文和畢馬威最近的一項調查顯示，超過 93% 的響應組織處理員工使用未經批准的個人設備和存儲或文件共享軟件來存儲公司數據 [6個].

世界上最大的 IT 從業者領導力調查也發現了 IT 部門之外控制的技術支出不可阻擋地增長，因為幾乎三分之二完全禁止業務管理 IT 的組織仍然報告其存在[7]. 由於許多接受調查的組織將缺乏安全控制和錯誤配置作為數據洩露的常見原因，因此超過四分之一的組織將未經授權使用雲服務視為他們對信息安全的最大挑戰 [6個]. 除了使組織面臨相當大的安全威脅外，四分之一的組織已經經歷過公共雲中的數據盜竊 [8個]，使用此類系統也可能會產生法律影響。許多公共雲服務不符合外部法規規定的數據主權監管要求，例如歐盟通用數據保護條例 (GDPR) [9]. 在此背景下，重要的是確保員工使用的雲服務符合內部和外部法規，並且不會使組織或其員工面臨風險。

為了解員工的行為，行為信息安全研究的重點是檢查正式製裁的影響（例如，罰款、減薪或負面績效評估）[10] 預計會鼓勵/阻止員工遵守/不遵守信息安全政策 [11]，主要採取威懾理論及其擴展的理論視角[12]. 然而，這些制裁的結果並不一致，有時

* 通訊作者。
*電子郵件地址：*lennart.jaeger@ebs.edu (L.耶格),andreas.eckhardt@ggs.de （A.埃克哈特），julia.kroenung@ebs.edu （J. Kroenung）。

https://doi.org/10.1016/j.im.2020.103318
2018 年 1 月 26 日收到；2020 年 4 月 7 日以修訂形式收到；2020 年 4 月 12 日接受 2020 年 5 月 17 日
在線提供

矛盾的，特別是當考慮到其他因素，如非正式製裁（例如，社會不贊成和自我不贊成）時[12]. 基於對犯罪學文獻的了解，我們認為，通過更密切地關注員工製裁預期的潛在調節作用，可以消除先前研究結果之間的差異，即正式和非正式製裁的影響可能不同質跨員工[12[13]. 威懾是指個體權衡風險和回報以決定是否冒犯的感知過程，而潛在不服從者參與這種計算的能力或意願是指個體的可威懾性[14].

早在 50 年前，犯罪學研究就批評說，很少有方法指出威懾措施的有效性與人員類別有關，因此與他們的不同威懾力有關 [15]; 關於個人如何看待和回應正式製裁，我們仍然知之甚少 [13]. Pogarsky [14, p. 14] 是為數不多的明確解決這個問題的學者之一。432]誰說“*懲罰威脅僅對總人口中的一小部分人產生影響*”直到今天，基於群體的方法來調查可遏制性在犯罪學領域仍然很少見，在信息安全研究中也不存在。目前尚不清楚制裁威脅響應能力如何影響意識和看法，從而影響可威懾性 [16]. 研究表明，政策可以操縱制裁威脅的看法 [17]. 政策是否影響個人的威脅感知還取決於他們對政策的態度。這些態度需要與對風險的態度區分開來 [18]，與違反政策的後果比政策本身更相關。因此，特別重要的是要專門觀察對政策的態度，這隱含地包括對其感知公正性的評估[19]和他們的創造者[20,21] 影響員工的威懾力。

在組織過程中實現合規和避免違反外部法規的潛在風險的重要步驟包括確保員工了解組織的政策、實踐和程序。因此，員工對雲使用政策的認識和遵守是信息安全經理最關心的問題之一 [22]. 但由於當今組織中的幾組員工傾向於繞過政策並使用未經批准的技術，因此非常重要的是要研究正式和非正式的製裁如何影響那些（不願意）遵守的員工群體，以及他們對此類政策的態度如何影響他們在這方面的威懾力。

因此，我們採用了 Pogarsky 提出並實施的基於組的方法 [14]，並通過檢查正式、社會和個人制裁對信息安全政策合規性的影響是否因員工對組織安全政策的積極或消極態度的不同程度而不同來調查員工的威懾性。因此，在這項研究中，我們解決了以下研究問題：*員工的威懾力在多級制裁與信息安全政策合規性之間的關係中起什麼作用？*

我們使用與在工作中使用公共雲服務相關的信息安全政策合規性調查來憑經驗測試我們的研究模型。我們調查了公共部門的 311 名員工，他們受組織的信息安全政策和 GDPR 監管，但在同事往往經常規避這些政策的環境中工作 [23–25]. 採用偏最小二乘多組分析 (PLS-MGA) 來檢驗對關係的調節作用。我們的研究通過引入可阻止性的概念，為有關員工信息安全政策合規性的文獻做出了貢獻。特別是，我們通過提供證據證明正式、非正式的社會和個人自我制裁的效果在很大程度上取決於員工對信息安全政策的態度，從而證實了可遏制性在行為信息安全研究中的作用和重要性。具體來說，根據我們基於群體的方法，

我們發現不同的員工群體遵守其公共部門組織中的政策。*傾斜的編譯器*(即，具有積極態度的員工隨後服從）是不可阻擋的，因為他們對正式的製裁不敏感，因為他們出於內心的信念而服從，而*不願遵守的人*(即，具有消極態度但仍然遵守的員工）是可威懾的。我們還發現，信息安全政策意識與傾向員工的個人自我制裁有更強的關聯，部分地與拒絕員工的正式和社會制裁有更強的關聯。這種關注個人威懾力的基於群體的觀點開闢了新的途徑來檢驗正式、非正式的社會和個人自我制裁在安全管理中的價值，並提供了對先前與威懾相關的信息安全研究的不一致結果的洞察。12].

二、研究背景

2.1. 威懾力和威懾力

威懾處理制裁威脅如何抑制犯罪或越軌行為，例如不遵守規則和政策。威懾被普遍認為是一種基於感知的現象，因為個人必須感知制裁威脅才會受到它們的影響 [26–28]. 因此，在威懾研究中，通常衡量製裁的感知狀態 [12]. 因此，經典的威懾理論集中在正式的製裁上，這些制裁被認為可以在某種程度上阻止犯罪，因為隨著個人感知到的確定性和懲罰的嚴重性增加，實施相應行為的可能性降低 [29]. 當代威懾理論通過解釋非正式製裁的作用（例如預期的社會反對和自我反對）作為法外合規來源擴展了經典框架 [30,31]. 對威懾理論的關鍵方面進行了大量的實證研究，並且在犯罪學和犯罪學方面都有詳盡的評論[30]和信息安全[12] 字段。一項重要發現是，制裁對合規行為的影響並非放之四海而皆準。相反，必須承認不同個人在製裁威脅方面存在的差異威懾力 [32].

在明確研究可遏制性的學者中，Pogarsky [14] 將可威懾性定義為對製裁威脅的反應，並將個人分為三種類型的決策者之一：敏銳的循規蹈矩者、可威懾者和不可救藥者。*頑固的墨守成規者*和*頑固不化的罪犯*是兩種不同類型的人，他們對正式製裁不敏感，而*威懾力*是對正式製裁的反應介於兩個極端之間的個人。敏銳的循規蹈矩的人是那些非正式的影響，例如社會不贊成和自我不贊成，已經確保服從的人。不可救藥的人是正式製裁無關緊要的個人，因為他們是頑固的罪犯，不受勸阻。可威懾者既不堅定地服從也不服從，隨著懲罰的確定性和/或嚴厲程度的增加，他們變得不太可能冒犯[14].

政策有能力影響個人對製裁威脅的看法[17]. 然而，這在很大程度上取決於個人對政策和違反政策的風險的態度 [18,20,21]. 因此，在下一小節中，我們開發了一個態度-遵從矩陣，突出了個人基於信息安全策略遵從性以及他們對其組織的信息安全策略的態度的威懾力。

2.2. 不願和傾向於遵從者

在信息安全背景下，政策是態度和行為所針對的關鍵對象之一 [33]. 根據 Eagly 和 Chaiken [34]， 僱員'*對信息安全政策的態度*描述他們對信息的評價傾向

他們組織的安全政策以及他們對這些政策的看法是有利還是不利。正如 Zhang 等人所定義的，我們將對信息安全策略的態度稱為對對象的態度。[35]和張、孫[36]，在概念上不同於對行為的態度，在我們的案例中，這是一種對行為順從的態度。張等。[35]和張、孫[36] 證明對於那些不同的態度概念化有不同的統計效果。薩法等人。[37]，例如，強調政策態度對合規行為的重要性。然而，Safa 等人。[37] 不在概念上區分對政策的態度和對合規行為的態度（見 [35]). 例如，積極的態度可能是對組織本身高度認同的原因 [38, 39] 或與信息安全政策的一般協議 [40]. 相比之下，對信息安全策略的消極態度可能導致人們普遍認為 IT 部門使用它們來控制員工開展信息相關工作的方式 [33].

關於基於員工對信息安全政策和信息安全政策合規性的態度來理解可阻止性，我們採用了 Pogarsky 所做的基於組的方法 [14] 在犯罪學研究中。因此，我們的結構化分析檢查了員工的態度行為關係，因為它與他們的傾向和後續行動有關。這種方法也適用於其他 IS 環境 [41].

在我們的研究中，我們觀察到信息安全政策遵從與積極和消極態度一致，以產生遵從傾向（即，主要基於員工對信息安全政策的態度，態度控制意圖）。我們採用這種觀點來更詳細地了解對兩個群體的可遏制性影響：傾向於和不傾向於的遵從者。此外，通過將態度定義為與先前研究一致的區分變量 [41]，我們避免了 Titah 和 Barki 所確定的態度和規範結構之間的非線性問題 [42] 如果這兩個構造被建模為相同的行為決定因素。

*傾斜的編譯器*是對遵守這些政策的信息安全政策持積極態度的員工。他們確信其組織的安全策略的公正性和有用性，並且願意並且能夠將它們轉化為與策略一致的行為。他們遵守這些安全政策，或者是因為他們評估政策的目標和意圖是積極的，因此分享它們（私人接受，參見 [43]), 或者甚至將它們作為自己的（強制性）目標，從而將它們內部化（內部化，cf [38]). 員工只會將安全政策相關的禁令和要求視為非強制性的，並在認為合適的情況下自願予以確認。在這種情況下，服從導致滿足，因此具有自我強化的特徵。這種個人行為幾乎不需要或不需要正式的製裁制度，因為個人主要是出於“內心的信念”而尋求遵守，而不考慮對後果的預期。因此，傾向於遵從的人代表了一種不可遏制的形式（即對正式製裁威脅不敏感）。他們服從是因為他們相信這是正確的做法，而不是因為他們害怕制裁威脅。類似於 Pogarsky 的 [14] “敏銳的循規蹈矩者”，傾向於遵守規則的人不易受到正式製裁，因為即使沒有更多的正式製裁，他們也不會違反政策。

*不願遵守的人*是遵守信息安全政策的員工，即使他們對這些政策持消極態度。這些是可能受到製裁威脅的員工。類似於 Pogarsky 的 [14] “威懾罪犯”，如果不是因為受到懲罰的威脅，不願意遵守的人通常會違反信息安全政策。他們因為外部壓力而遵守政策，但不一定分享政策的基本目標和意圖。因此，他們遵守的原因在於不遵守行為的（預期的）不利後果（即害怕正式/非正式的製裁）。換句話說，他們遵守安全政策以避免受到懲罰，但並不私自接受。對於這個群體，正式的製裁制度是有效的，包括高檢測確定性，嚴懲違規行為。在社會制裁系統中，員工的行為部分取決於員工業務社交網絡中重要成員（例如，同事或團隊領導）的認可或反對，並且制裁通常是非正式的。如果由於缺乏監督或社會壓力而減少恐懼，合規水平可能會下降，因為員工會根據自己對這些政策的消極態度行事。

我們預計大多數員工不會因為嚴重的違規行為而“進入市場”，並且在考慮嚴重的系統濫用行為時，他們傾向於遵守規則。然而，當涉及到輕微的違規行為（例如，記下密碼、無法註銷或使用公共雲服務）時，更多的人處於這類行為的邊際，而且實際上是可以阻止的。問題通常不在於員工是不可救藥的違法者 [14] 打算傷害他們的組織，而是他們沒有足夠的動力去遵守信息安全政策 [4個]. 因此，研究人員和從業人員面臨著如何激勵員工從事良好的安全相關行為的重要問題 [2個,44]. 在此背景下，採用安全政策合規等積極結果變量的威懾研究通常表明，與 IS 濫用等消極結果變量相比，制裁的威懾效果較弱 [12]. 據此，一些學者質疑威懾理論對預測積極用戶行為的適用性，並呼籲進一步研究澄清這個問題[12]. 我們通過檢查傾向於和不願意的合規者來響應這一呼籲，以確定制裁可以促進理想合規性的員工子群體以及他們可能無效的子群體。

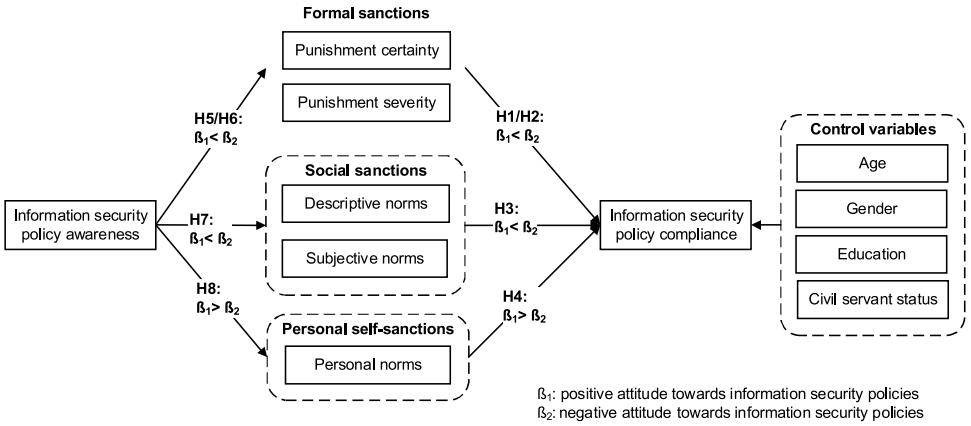
三、研究模型與假設

在本節中，我們介紹了我們的研究模型並討論了我們的假設。借鑒前一節中對（不）傾向的服從者的概念化，我們假設外部施加的激勵因素（正式和非正式的社會制裁）和自我施加的激勵因素（個人自我制裁）對行為的影響存在差異。員工對信息安全政策持積極或消極態度的信息安全政策合規性，ß1個和ß2個， 分別。我們還假設員工的多級制裁感知受其信息安全政策意識的影響。圖。1介紹我們的研究模型。

根據之前的研究 [12,45]，我們定義*信息安全政策合規*作為員工遵循這些組織政策以在工作中適當使用 IS 的程度。組織安全策略是指關於員工在正確使用和保護組織 IS 資源方面的角色和責任的正式指南 [2個,3個] 並傾向於嚴重依賴嚴格的行業和/或政府法規 [46]. 因此，檢查內部人員的信息安全政策合規性可以評估員工是否遵守這些政策中正式指定的角色和職責 [46]. 在我們的研究中，我們關注關於公共雲使用的信息安全政策作為一種信息安全政策。通過在未經 IT 部門正式批准的情況下使用公共雲系統（例如 Dropbox），員工通常會違反其組織的信息安全政策 [5個]. 兩位學者[5個]和從業者[8個] 將此違規視為組織的信息安全問題，它會帶來重要的信息安全威脅，例如數據盜竊或違反法規。在以下小節中，我們詳細介紹了模型構造並描述了它們的假設。

3.1. 正式製裁

正式製裁代表因某些形式的不合規行為而導致的明確懲罰（例如，罰款、減薪或負面績效評估）[47]. 例如，將組織文檔存儲在



圖。1。研究模型。

未經授權的外部雲系統可能會導致員工被解僱 [48歲]. 關於威懾的犯罪學研究將正式製裁概念化為感知到的懲罰的嚴重性和確定性，在組織環境中，它已經被重新定義並適應因被禁止的工作場所行為而被抓獲和懲罰 [49]. 儘管犯罪學中的威懾理論和組織環境中的實證支持具有強大的理論基礎 [30,31]，信息安全文獻在解釋支持（例如，信息安全策略合規性）或破壞信息安全（例如，IS 濫用）的用戶行為時產生了不同的發現[12, 50]. 一些研究為威懾理論的基本原理提供了實證支持（例如 [51]), 而其他人僅報告部分支持（例如 [52,53]). 儘管在信息安全領域存在部分矛盾的發現，但威懾理論被認為是一種被廣泛接受的理論，並且研究威懾措施未發揮應有作用的原因被認為是一項重要的努力 [33]. 因此，根據現有研究，我們應用（感知） *處罰力度*和*懲罰確定性*作為對從事不合規行為的正式製裁的組成部分。

雖然大多數關於行為信息安全的研究都沒有解決正式製裁的威懾效果是否對員工不同的問題，但犯罪學研究結果表明，制裁的影響因人而異 [30,54]. 例如，關於稅收遵從的實證研究結果表明，正式製裁對那些對稅法持消極態度的個人的稅收作弊具有更大的威懾作用，因此可能更有動機作弊 [55]. 因此，根據我們的概念化 *不願遵守的人*在部分2個，我們假設正式製裁預期是信息安全政策合規性的核心，因為當員工對這些政策持消極態度並因為害怕因不合規而受到正式製裁而遵守這些政策時。例如，當員工預計使用公有云服務的懲罰的嚴重性和確定性會很高時，他們會遵守雲使用政策，儘管他們不願意這樣做以避免後果。因此，我們假設：

H1. 懲罰c確定性有一個gr 與傾向於的員工相比，不願意的員工對信息安全策略合規性的影響更大。

氟氣. 懲罰嚴重程度對信息安全策略合規性影響更大
不情願 d 員工比 for 傾斜
僱員。

3.2. 社會制裁 秒

此外 正式製裁， 當代威懾研究

還認識到行為的社會調節後果的作用，或者換句話說，非正式的社會制裁[30]. 從威懾的角度來看，個人預期行為後果的主觀價值不僅受到正式製裁（如罰款）的影響，還受到非正式社會制裁的影響[31]. 非正式社會制裁的一個例子是社會不贊成，其中包括那些意見被個人看重的人的譴責 [56]. 在組織環境中，這可能是從同行或領導那裡收到的違反信息安全政策的負面反饋。社交網絡中重要成員對不服從行為的負面反應增加了不服從行為的心理成本，從而降低了其吸引力[57]. 如果社會規範被定義為（主要是隱含的）關於如何行為的規則和標準[34]，很明顯，它們可以以不同的方式規範行為，儘管它們沒有表達為正式的法律或法令。社會規範包括通過批准或獎勵和拒絕或懲罰以社會制裁形式出現的評估成分。

有兩種主要類型的社會規範[58]：描述性和主觀性。*描述性規範*根據自己對其他人在類似情況下的行為方式的看法，提供有關什麼是最合適的行為的信息。*主觀規範*另一方面，根據員工對其職業社交網絡中重要成員（例如，同事和主管）會贊成或不贊成的期望，具體說明員工應該如何行事。描述性規范代表（不確定）情況下的重要社會信息，而主觀規範描述了通過社會過程通過承諾獎勵（社會認可）或懲罰（社會不認可）來調節群體行為的規範規則[59]. 多項研究記錄了社會規範對信息安全政策合規和不合規行為的影響[53,58, 60].

在強制性設置中，政策規定應該或不應該如何使用焦點系統，社會規範已被證明主要通過合規機製而不是內化或識別來影響系統使用決策 [61]. 雖然內化和認同與個人信念結構的改變有關，但服從機制導致員工僅僅為了應對社會壓力而改變他們的行為，即員工遵守社會規範，特別是當重要的社交網絡合作夥伴能夠獎勵時期望或懲罰不期望的行為[62]. 根據我們在部分中對不願遵守的人的論證2個，我們認為非正式的社會制裁期望

社會規範中固有的，並通過主觀和可操作的
描述性的 orms 是信息安全策略合規性的核心
當僱用 當員工認為沒有其他人使用 unaulic 雲服務來存儲組織數據
政策。塔 時，他們對信息安全持消極態度
酒吧

同事或其他人希望個人遵守組織的雲使用政策，儘管他們不願意，但他們會遵守該政策以避免社會不贊成（例如，負面反饋）。因此，我們假設：

H3. 社會規範對不情願員工的信息安全政策合規性的影響大於對情願員工的信息安全政策合規性。

3.3. 個人自我制裁

雖然員工可能知道一種規範，甚至相信這是一種由他人持有並與社會獎懲相關的社會規範，但他們可能對它沒有什麼個人依戀。因此，有必要考慮外部規範在多大程度上也是 *個人規範*，即與個人的自我概念相關並被體驗為執行或避免某些行為的道德義務感的規範[63]. 與通過社會反對來強制執行的社會規範相反，個人規範的執行是通過發自內心的自我反對來實現的。自我否定包括“對法律合法性的信念、對法律規範的道德承諾、規範的內化和良心”（[64，頁。432] 引自 [14]). 在組織環境中，這可能涉及員工認為違反信息安全政策是一件嚴重的事情，或者對他或她來說是不可接受的。隨之而來的是，某些不合規行為沒有被實施，因為它們被認為是錯誤的 [30]. 犯罪學研究的結果表明，個人規範或道德標准在很大程度上決定了個人實施非法行為的意圖，例如公司犯罪 [31] 或逃稅 [56]. 儘管個人規範在支持信息安全的行為研究中沒有受到廣泛關注，但一些研究表明，個人規範直接對信息安全政策遵守意願產生積極影響[65] 或間接通過對安全相關行為的態度 [66,67].

因此，當信息安全策略被內化為員工道德推理的一部分時，他們可能會覺得更有義務將其轉化為與信息安全策略一致的行為。根據我們對傾斜遵從者的概念化，我們期望信息安全政策與員工道德價值觀之間的一致性 [31] 對信息安全政策持積極態度的員工會更強大。例如，當員工認為將與工作相關的文檔保存在公有云系統中違反雲使用政策是一件嚴重的事情或不可接受時，他們會根據自己的意願遵守政策，避免自我否定。因此，我們假設：

H4. 個人規範對傾向於員工的信息安全策略合規性的影響大於不傾向於員工的信息安全策略合規性。

3.4. 信息安全政策意識

信息安全策略意識被定義為員工對組織信息安全策略中規定的要求以及這些要求的目的的知識和理解[2個]. 這個定義基於這樣的概念，即意識是一種狀態，在這種狀態下，員工意識到並理想地致力於組織的信息安全目標，正如信息安全政策中經常表達的那樣[68]. 我們建議信息安全策略作為影響員工多級制裁感知的重要信息基礎。

首先，信息安全政策依賴於與社會法律相同的威懾機制，通過提供關於什麼是不良行為的信息並增加對此類行為的製裁威脅感知 [52,69]. 特別是，員工對信息安全政策的意識增加了感知懲罰的確定性，因為政策意味著通過組織執行的存在安全努力（例如，監視和檢測活動），以及感知到的懲罰嚴重程度，因為政策表明將對違反政策的行為施加懲罰[52].

其次，信息安全政策可能會影響組織內與政策相關的社會規範。制定和實施信息安全政策的組織通過安全教育、培訓和意識計劃等各種渠道向員工發出期望信號，以確保信息安全政策意識和合規性[70]. 這種期望會影響員工關於信息安全政策的規範。例如，員工認為他們的組織通常重視其信息安全政策所指示的遵守規則的行為，他們更有可能相信他們的大多數同事要么遵守這些政策，要么期望他們遵守 [71]. 因此，信息安全策略的意識有助於提供有關描述性和主觀規範的相關想法。

第三，信息安全政策代表了某種組織要求，其中還包括承諾和內部化 [68]. 組織希望他們的員工內化並遵守信息安全策略，而不是僅僅知道但不應用它們。具有信息安全政策意識的員工會將政策視為他們必須遵守的事情。這種承諾可以是外部或內部動機[68]. 該義務屬於角色責任和/或道德責任範疇[68,72]. 角色責任不同於道德義務（或個人規範，見上一節）的感受。責任與員工的組織職責相關，例如認為自己有責任加強組織的信息安全。另一方面，道德義務與員工的感覺有關，他/她應該按照他/她的價值體系行事，例如認為自己在道德上有義務遵守信息安全政策，因為遵守規則是一個人價值體系的一部分[71]. 然而，道德義務感的程度也是責任的函數[63]. 因此，個人對規定責任的信息安全政策的意識導致了與政策相關的個人規範的形成。

一方面，對信息政策持積極態度的員工（有傾向的員工）認為這些政策是可以接受的和可取的，因此更有可能承認增強組織信息安全的責任感與對信息政策的道德義務感之間的聯繫。信息安全策略合規性。因此，對信息安全政策的積極態度有助於信息安全政策意識成功轉變為與政策相關的個人規範。

另一方面，對信息安全政策持消極態度的員工（拒絕員工）將他們的目標和意圖評估為消極的，因此不會分享或私下接受它們。這種消極態度使員工可以證明拒絕承擔責任無視他們的道德義務[73]. 因此，消極態度會抑制信息安全政策意識向政策相關個人規範的轉變。在這種情況下，他們的承諾仍然是外部的，作為一種遵守的動機[68]. 當他們的行為不符合他們正式要求或社會期望的角色時，他們的角色責任感將通過正式製裁和非正式（社會）制裁的感知風險來傳達。因此，他們會將信息安全政策更多地視為與獎勵和懲罰（有形或社會）相關的外部角色績效評估的基礎，而不是內部的羞恥感或反對感。換句話說，不願意的員工比願意的員工更容易接受雲使用政策中固有的信息，即會受到製裁，而其他人會不贊成違規行為。因此，我們建議：

H5. 信息安全政策意識對消極員工的懲罰確定性的影響大於傾向員工。

H6. 信息安全政策意識對企業的影響更大

對不情願的員工的懲罰比對不情願的員工的懲罰更嚴厲。

H7. 信息安全政策意識對不積極員工的社會規範的影響大於對不積極員工的社會規範的影響。

H8. 信息安全策略意識對傾向性員工的個人規範的影響大於對傾向性員工的個人規範的影響。

3.5. 控制變量

根據信息安全文獻，我們在研究模型中包含了幾個控制變量。這些變量包括個體差異因素，例如*年齡*[52],*性別*[58],*教育*[74]， 和*公務員身份*.

四、研究方法

我們進行了一項調查來檢驗這些假設。對於試點調查，我們首先根據文獻確定並製定了合適的措施。我們對幾個目標受眾成員進行了試點調查，然後完善了在線管理的最終調查。在以下小節中，我們將討論儀器開發並描述數據收集過程。

4.1. 儀器開發

構建體的測量項目以現有文獻為基礎，以提高結果的可靠性。表格1介紹項目的運作。捕獲正式製裁（通過懲罰嚴重程度和懲罰確定性操作）和非正式社會制裁（通過主觀和描述性規範操作）的項目改編自 Herath 和 Rao [58]. 捕捉個人自我制裁（由個人規範操作）的項目改編自 Ifinedo [66]. 捕獲信息安全策略意識的項目改編自 Bulgurcu 等人。[2個]. 儘管許多研究使用行為意圖作為內生變量，但我們考慮的是自我報告的行為，因為自我評估通常比意圖更容易 [75]. 一些實證研究（例如 [76,77],) 通過詢問員工的信息安全策略合規性來選擇這種方法。因此，捕獲信息安全政策合規性的兩個項目衡量了員工在工作中使用公共雲系統的政策合規程度。對於其中的每一項，受訪者使用李克特七分制量表評估了他們同意/不同意的程度，範圍從非常不同意 (1) 到非常同意 (7)。用於將樣本分成兩組的項目信息安全政策態度測量了受訪者對 Eagly 和 Chaiken 定義的目標的態度 [34]，特別是關於使用公共雲服務的政策，從非常消極 (1) 到非常積極 (7)。措施的對像是具體的單數，這意味著它由一個對象組成，這裡是公共雲政策，它很容易和統一地想像，從而支持使用單項措施而不是多項措施 [78]. 兩組在七分制量表的中立位置 (4) 中間分開。

4.2. 數據採集

該調查是在德國公立大學的員工中進行的，內容涉及與使用雲服務相關的合規行為。大學僱員受僱於國家，因此是公共部門的一部分，公共部門有嚴格的隱私規定，旨在保護其公民。此外，員工受數據保護法的約束，大學的中央數據保護機構以信息安全和隱私問題為由禁止使用 Dropbox 等公共雲存儲服務。進行了基於網絡的調查以收集數據和

表格1
測量項目。

物品		規模[A]	意思是	標清
描述性規範 (DN)				
DN1	我相信其他員工遵守公共雲使用政策，不使用 Dropbox 等服務處理與工作相關的數據。我確信其他員工在工作中使用公有云服務，例如	A	2.95	1.77
DN2	Dropbox。	乙	2.83	1.78
DN3	很可能大多數其他員工遵守使用公共雲服務的政策，不使用 Dropbox 等服務來確保數據安全和保護。	A	3.23	1.76
信息安全政策態度（ATT） ATT1				
	我覺得……關於在工作中使用公共雲服務的政策。	C	3.84	1.74
信息安全政策意識（ISPA） ISPA1				
	我知道我的組織使用公有云的政策規定的規則和條例。	A	3.23	1.78
ISPA2	我了解我所在組織的公有云使用政策規定的規則和條例。	A	2.64	1.48
ISPA3	我知道我在公共雲使用政策中規定的責任，以增強我所在組織的信息安全。	A	1.77	1.11
信息安全政策合規性 (ISPC) ISPC1				
	我在工作中遵守公共雲使用政策。	A	4.58	1.81
ISPC2	我遵守有關在工作中使用公共雲的政策，不將與工作相關的文檔保存在公共雲服務（例如 Dropbox 或類似服務）中。	A	4.14	1.94
個人規範（PN）				
PN1	如果我不遵守雲服務使用政策和將工作相關文件保存在公共雲服務中，那將是一個嚴重的問題。	A	4.79	1.84
PN2	對我來說，忽視我的組織關於公共雲服務使用的政策是不可接受的。	A	4.64	1.93
PN3	對我來說，使用公共雲服務（例如 Dropbox）是一件小事。	乙	3.95	1.87
懲罰確定性（PC） PC1				
	我因違反公共雲服務政策而受到製裁的可能性很低。不太可能檢測到使用公共雲服務。	乙	2.59	1.42
PC2		乙	2.54	1.39
PC3	我的組織監控雲使用政策的合規性。	A	3.13	1.76
處罰嚴重程度（PS） PS1				
	如果我的組織知道我的行為，我會受到紀律處分。	A	3.45	1.53
PS2	我的組織懲罰違反雲服務使用政策的員工。使用公共雲服務（例如 Dropbox、Microsoft OneDrive	A	2.8	1.34
PS3	和 Google Drive）獲取工作相關數據等違規行為不會在我的組織受到處罰。	乙	3.31	1.75
主觀規範 (SN)				
SN1	我的老闆認為我應該遵守使用雲服務的政策。	A	5.11	1.79
SN2	我的同事認為我應該遵守使用雲服務的政策。	A	4.36	1.82
SN3	我所在組織的 IT 部門認為我應該遵守使用雲服務的政策。	A	3.72	1.99

[A]A：範圍從 1 = 非常不同意到 7 = 非常同意；B：同A，但項目反編碼；C：範圍從 1 = 非常消極到 7 = 非常積極。

相應的鏈接已通過電子郵件分發給國立大學的員工。作為完全自願和匿名參與的回報，完成調查並選擇參加抽獎的人抽取了五張在線零售商代金券。由於我們在本研究中的目的是探索對信息安全政策持不同態度的個人，因此我們的樣本由 311 名持正面或負面態度的參與者組成

對信息安全政策的態度。由於態度的平均值為 3.84（SD 1.74），這表明參與者對這些政策有輕微的消極態度，表明他們不願意遵守。態度量表近似對稱，偏度值為 0.03 (SD 0.13)，但峰度值為 -1.03 (SD 0.26)，這表明我們的樣本分佈不均，並強調需要進行特定於群體的分析。

表 2展示了我們兩個群體的人口特徵：積極的信息安全政策態度組和消極的信息安全政策態度組。在參與者中，99 人 (31.7%) 為女性，209 人 (67.0%) 為男性。大多數受訪者年齡在 22 至 40 歲之間 (71.4%)。大多數參與者擁有大學學位 (81.7%)，沒有公務員身份 (84.0%)，並在其機構的學術部門工作 (82.7%)。他們在所在機構的平均工作年限為 5.17 年（SD = 6.21 年）。

五、數據分析及結果

在我們的數據分析中，我們採用了偏最小二乘法 (PLS) 方法，這是一種用於測量測量模型和結構模型的常用回歸技術 [79]. PLS 對小樣本產生可靠的結果，可用於測試和驗證解釋模型 [79]. 為了檢驗我們的假設，我們通過進行基於引導的 PLS 多組分析來測量具有積極或消極態度的兩組員工的路徑係數差異 [80] 使用 SmartPLS 版本 3 進行 PLS 路徑建模。最初，評估了兩組測量模型的可靠性和有效性，然後評估了用於假設檢驗的結構模型。

5.1. 測量模型測試

為了評估測量模型，我們檢查了結構可靠性、指標可靠性、收斂有效性和區分有效性。結果顯示在表3. 使用複合可靠性 (CR) 評分評估結構可靠性 [81]. CR 值範圍從 0.7 到 0.96，超過了推薦的閾值 0.7 [81]. 通過檢查每個指標的構建負載來評估指標可靠性。高於閾值 0.6 的載荷可確保足夠高的指標可靠性 [82]. 為了評估收斂有效性，我們計算了提取的平均方差 (AVE) [83]. 每個潛在的 AVE 變量範圍從 0.55 到 0.92，高於建議的閾值 0.5。對於區分有效性的評估，我們考慮了 Fornell-Larcker 標準和交叉載荷 [81,82]，以及最近提出的異性-單性比（HTMT）測試[84]. 如圖所示表3, 每個構造的 AVE 的平方根高於構造之間的相關係數 [81,83]. 使用交叉負載的進一步評估證實了 Fornell-Larcker 標準的分析結果，因為所有指標在各自結構上的負載均高於其他結構。此外，更嚴格的 HTMT 比率證明了區分有效性，因為我們構造的所有 HTMT 值都小於 0.9 [84,85] 並且根據 HTMT 推斷的統計檢驗與 1 顯著不同（即，通過自舉得出的置信區間都不包含值 1 [84]). 因此，區分有效性的三個標準得到滿足，表明我們對模型中所有結構的測量彼此不同。

最後，為了評估共同方法方差 (CMV)，我們使用了標記變量技術 [86,87]. 我們選擇了受訪者的個人創新能力，這是通過從 Agarwal 和 Karahanna 中提取的三個項目來衡量的 [88]，作為標記變量及其與研究中其他變量的平均相關性（$r_{米}$=0.098 和$r_{米}$=積極和消極信息安全政策態度組分別為 0.095）用作 CMV 估計。我們計算了 CMV 調整後的相關性和*嚇*-統計數據 [87]. 對於積極和消極的信息安全政策態度組，這種調整導致的相關性平均變化分別為 0.071 和 0.078。顯著性檢驗的結果表明，在控制 CMV 後，未校正的顯著相關性都沒有變得不顯著，這表明 CMV 偏差不太可能成為本研究的關注點。

5.2. 結構模型測試

為了評估結構模型，我們檢查了 $R_{2個}$路徑係數的值和估計。我們發現我們的模型分別解釋了 51.2% 和 47.6% 的積極和消極態度員工的信息安全政策遵守方差，表明外生變量具有適度的解釋力 [79].

為了檢驗我們的假設，我們進行了 PLS-MGA [80]. 通過應用 PLS-MGA，我們可以針對不同的先驗指定群體測試相同模型之間的顯著差異，在我們的例子中，這些群體是對信息持積極或消極態度的員工

表 2
樣本的人口統計特徵。

		積極的信息安全政策態度（*n*=141)		消極的信息安全政策態度（*n*=170)	
措施	物品	數數	%	數數	%
性別	女性	35	24.8	63	37.1
	男性	104	73.8	105	61.8
	未指定	2個	1.4	2個	1.2
年齡（歲）	18- 20	2個	1.4	7	4.1
	21- 30	54	38.3	71	41.8
	31- 40	46	32.6	52	30.6
	41- 50	24	17.0	26	15.3
	51- 60	11	7.8	12.	7.1
	> 60	3個	2.1	2個	1.2
	未指定	1個	0.7	0	0
最高學歷	普通中學 中學 特殊高中 文法學校	0	0.0	1個	0.6
	課程 A-level 大學學位	0	0.0	3個	1.8
		1個	0.7	3個	1.8
		14	9.9	20	11.8
		116	82.3	138	81.2
	其他學位	10	7.1	5個	2.9
公務員身份	是的	29	20.6	19	11.2
	不	112	79.4	149	87.6
	未指定	0	0.0	2個	1.2
職業	學術部門	127	90.1	130	76.5
	行政部門 未指定	13	9.2	30	17.6
		1個	0.7	10	5.9

表3
測量模型。

積極的信息安全政策態度(*n*=141)

構造	加載量	鉻	AVE	AVE 和 HTMT 值的互相關和平方根（括號內）[b] 12345					6個	7
1.描述性規範	0.88– 0.91	0.90	0.75	**0.86**						
2.信息安全政策意識	0.60– 0.88	0.70	0.55	0.41 (0.47)	**0.74**					
3.信息安全政策合規	0.95– 0.97	0.96	0.92	0.13 (0.29)	0.40 (0.79)	**0.96**				
4.個人規範	0.85– 0.92	0.93	0.81	0.42 (0.49)	0.32 (0.62)	0.69 (0.76)	**0.9**			
5. 處罰確定性	0.62– 0.87	0.81	0.59	0.34 (0.43)	0.16 (0.45)	0.29 (0.34)	0.30 (0.36)	**0.83**		
六、處罰力度	0.67– 0.94	0.79	0.66	0.46 (0.63)	0.24 (0.67)	0.32 (0.41)	0.38 (0.48)	0.56 (0.82)	**0.81**	
7.主觀規範	0.71– 0.99	0.87	0.77	0.24 (0.25)	0.36 (0.79)	0.32 (0.29)	0.36 (0.34)	0.29 (0.37)	0.37 (0.52)	**0.88**

消極的信息安全政策態度(*n*=170)

構造	加載量	鉻	AVE	AVE 和 HTMT 值的互相關和平方根（括號內）[b] 12345					6個	7
1.描述性規範	0.90– 0.93	0.94	0.84	**0.91**						
2.信息安全政策意識	0.70– 0.81	0.72	0.57	0.48 (0.56)	**0.75**					
3.信息安全政策合規	0.91– 0.92	0.92	0.84	0.33 (0.70)	0.18 (0.38)	**0.92**				
4.個人規範	0.78– 0.84	0.86	0.67	0.14 (0.16)	0.00 (0.1)	0.45 (0.56)	**0.82**			
5. 處罰確定性	0.73– 0.80	0.86	0.75	0.25 (0.32)	0.37 (0.86)	0.21 (0.28)	0.13 (0.18)	**0.87**		
六、處罰力度	0.78– 0.88	0.81	0.69	0.25 (0.34)	0.21 (0.49)	0.35 (0.50)	0.20 (0.31)	0.26 (0.38)	**0.83**	
7.主觀規範	0.87– 0.95	0.91	0.83	0.21 (0.23)	0.16 (0.36)	0.46 (0.55)	0.35 (0.41)	0.24 (0.31)	0.26 (0.38)	**0.91**

[b]對角線（粗體）上的值顯示 AVE 的平方根，而對角線外的值是潛在結構之間的相關性。HTMT 值顯示在括號中。

安全政策。與一次檢查單個結構關係的測試調節的標準方法不同，PLS-MGA 是一種簡單、直接且有效的方法，可以同時評估所有模型關係的調節 [89,90 後]. 此外，如果將亞群視為單個同質組，則可以使用已識別的差異來突出潛在錯誤，因為這些差異在作為一個整體進行研究時可能並不明顯 [91]. 最後，通過深入了解群體差異，基於結果的策略實施（例如，政策和培訓計劃）可以更具體地針對異質群體 [89].

在比較組特定路徑係數之前，我們需要評估測量不變性 [92]，這為我們的發現增加了額外的準確性 [89]. 使用複合模型 (MICOM) 評估的測量不變性，我們建立了部分測量不變性（見附錄 A），這使我們能夠比較路徑係數 [92].

接下來，我們估計兩組的 PLS 結構模型，包括路徑係數和顯著性水平（見第三和第四列表 4). 每組都用 5000 個 bootstrap 樣本進行 bootstrap 分析。然後，每個路徑係數對信息安全政策持積極態度的群體的估計（$ß_{1個}$) 與那些對信息安全政策持消極態度的人的估計 ($ß_{2個}$). 正差和零差的數量除以比較總數表示$ß_{1個}$大於$ß_{2個}$. 結果在 5% 的水平上顯著，如果*p*-值小於 0.05 或大於 0.95 [80]. PLS-MGA 的結果在第五列 表 4.

關於正式製裁，我們發現對於不願意的員工來說，懲罰嚴重程度和信息安全政策合規性之間的路徑明顯更強（$|ß_{1個}-ß_{2個}| = 0.17, p<0.05$），但不是從懲罰確定性到信息安全策略合規性的路徑。因此，我們找到了支持 H2 但不支持 H1 的證據。在非正式（社會）制裁方面，描述性規範的影響存在顯著差異（$|ß_{1個}-ß_{2個}| = 0.25$，$p<0.01$) 和主觀規範 ($|ß_{1個}-ß_{2個}| = 0.18, p<0.05$) 對信息安全策略的遵從性，這兩者對於不情願的員工來說都更強。因此，我們找到了支持 H3 的證據。對於個人自我制裁，從個人規範到信息安全政策合規的路徑對於有傾向性的員工來說明顯更強（$|ß_{1個}-ß_{2個}| = 0.32$，$p>0.999$);

表 4
多組分析測試結果。

	小路[c]	係數		PLS-MGA	
		積極的安全政策態度（$ß_1$個）	消極的安全政策態度（$ß_2$個）	係數差異 ($|ß_{1個}- ß_{2個}|$)	假設
正式製裁	個人電腦→ISPC	0.07 納秒	0.02 納秒	0.05 納秒	H1：$ß_{1個}<ß_{2個}$(拒絕了）
	聚苯乙烯→ISPC	− 0.04 納秒	0.13*	0.17*	假設2：$ß_{1個}<ß_{2個}$（支持的）
非正式製裁	DN→ISPC	0.12 納秒	0.36***	0.24**	H3：$ß_{1個}<ß_{2個}$（支持的）
	序列號→ISPC	0.06 納秒	0.23**	0.18*	
自我制裁	公稱→ISPC	0.60***	0.28***	0.32***	H4：$ß_{1個}>ß_{2個}$（支持）
	國際空間站→個人電腦	0.16*	0.37***	0.22*	H5：$ß_{1個}<ß_{2個}$（支持）
	國際空間站→聚苯乙烯	0.24***	0.21***	0.03納秒	H6：$ß_{1個}<ß_{2個}$（拒絕）
信息安全政策意識	國際空間站→DN	0.13 納秒	0.33***	0.19*	H7：$ß_{1個}<ß_{2個}$（部分支持）
	國際空間站→序列號	0.36***	0.16*	0.20*	
	國際空間站→公稱	0.19*	− 0.08 納秒	0.28**	H8：$ß_{1個}>ß_{2個}$（支持的）

*** $p<0.001$。
** $p<0.01$。
* $p<0.05$，ns = 不顯著。
[c]ISPC = 信息安全政策合規性，PC = 懲罰確定性，PS = 懲罰嚴重程度，DN = 描述性規範，SN = 主觀規範，PN = 個人規範，ISPA = 信息安全政策意識。

因此，我們的證據支持 H4。在信息安全政策意識方面，從意識到懲罰確定性的路徑對於不願意的員工來說明顯更強（$|\beta_{1個} - \beta_{2個}| = 0.22$，$p<0.05$），但不是從意識到懲罰嚴重程度的路徑。因此，我們的證據支持 H5 而不是 H6。從信息安全策略意識到描述性規範的路徑對於不願意的員工來說要強得多（$|\beta_{1個} - \beta_{2個}| = 0.19, p<0.05$），但不是從意識到主觀規範的路徑。因此，我們的證據為 H7 提供了部分支持。正如預期的那樣，從信息安全政策意識到個人規範的路徑對於有傾向性的員工來說要強得多（$|\beta_{1個} - \beta_{2個}| = 0.28, p>0.992$）; 因此，我們的證據支持 H8。最後，在測試我們的結構模型時，根據信息安全文獻考慮了信息安全政策合規性的幾個控制變量（年齡、性別、教育水平和公務員身份）2個,52,58]. 兩組均無顯著性差異，並且基於 PLS-MGA 也無顯著差異。

為了檢查我們結果的穩健性，我們還考慮了 PLS 路徑模型中遺漏變量可能產生的內生性。我們在附錄 B 中對內生性的評估遵循 Hult 等人的 [93] 解決偏最小二乘結構方程模型 (PLS-SEM) 中內生性的系統程序，表明不存在內生性，這支持了結構模型結果的穩健性 [93].

6.討論

在本文中，我們應用基於組的方法來檢查可阻止性 [14] 通過採用將正式、社會和個人制裁與信息安全政策意識相結合的安全政策合規模型。我們測試它們的影響是否根據員工對信息安全政策的積極或消極態度的程度而有所不同。在下文中，我們將討論我們的主要發現、它對理論和實踐的影響，以及進一步研究的局限性和有趣的途徑。

6.1. 主要發現

我們的結果證實了可阻止性在信息安全研究中的作用和重要性，發現根據員工對信息安全政策持積極或消極態度分組的信息安全政策遵從性受到外部施加（正式和非正式社會制裁）的不同影響) 和內部施加的（個人自我制裁）激勵力量。

具體來說，我們基於群體的方法表明，有傾向的員工（即態度積極的員工）的信息安全政策合規性主要是由他們的個人規範 (H4) 驅動的，而不是由對正式製裁 (H1、H2) 或非正式社會的看法驅動的制裁 (H3)。這些發現為我們對傾向性遵從者的概念化提供了強有力的支持。特別是，類似於敏銳的墨守成規者 [14]，他們無法被嚇倒，因為他們對正式製裁不敏感。相反，他們的信息安全策略合規性在很大程度上取決於他們自己對行為是否適當的個人信念。這種內部驅動因素是可持續的，因為無論制裁預期如何，它都會存在。我們還發現信息安全政策意識與傾向員工的個人規範有更強的關聯 (H8)。因此，了解信息安全策略中規定的責任會導致這些員工產生道德義務感。

我們的結果還表明，不願意遵守的人（即那些態度消極但仍然遵守的人）是可以威懾的。然而，當員工對信息安全政策持消極態度時，正式製裁的威懾作用主要通過懲罰嚴重程度 (H2) 而不是懲罰確定性 (H1) 發揮。此外，非正式社會制裁的威懾作用顯現在他們的合規中發揮重要作用。這意味著，儘管這些不願遵從的人可能對信息安全政策的印像不太積極，也不太願意遵守這些政策，但他們會改變自己的行為以遵守同事的行為（即描述性規範），以及主管和同事的期望（即主觀規範）（H3）。我們的研究結果與犯罪學文獻一致，其中發現非正式的社會制裁比正式的社會制裁對越軌行為具有更強的威懾作用 [94]. 最後，我們發現信息安全政策意識對正式和非正式（社會）制裁感知的部分支持對於不願意的員工來說更強。關於正式製裁，我們發現意識對懲罰確定性的影響不同，對於不願意的員工來說路徑更強 (H5)，但懲罰嚴重程度 (H6) 沒有顯著差異。然而，嚴重程度對合規性的後續差異影響對於不願意的員工來說更強，這表明信息安全策略意識影響信息安全策略合規性的基礎過程存在差異。在非正式（社會）制裁方面，正如預期的那樣，信息安全政策意識與不情願員工的描述性規範有更強的關聯，但與預期相反，與主觀規範的關聯較弱 (H7)。一種可能的解釋是，不願意的員工可能已經從他們自己對信息安全政策的消極態度概括為更大群體的觀點，從而對其他人的期望產生錯誤的共識效應 [95]. 個人可能會投射他們的觀點，因為他們對普遍的主觀規範知之甚少，但他們非常了解自己的觀點。

6.2. 理論貢獻

在本文中，我們考慮了製裁影響信息安全策略合規性的條件。特別是，我們專注於理解威懾力的概念，以檢查哪些員工子群體制裁實際上可以發揮有用的威懾效果，哪些不能。

為了區分三種不同類型的製裁的威懾效果，我們研究了兩個具有不同威懾力的群體：態度積極但隨後遵守的員工（“傾向遵守者”）和態度消極但仍然遵守的員工（“拒絕遵守者”）. 區分這兩組提供了對早期信息安全研究中製裁的威懾作用（或缺乏威懾作用）的不一致結果的初步解釋。具體來說，雖然質疑的研究得出的結論不一致（例如，[53,96,97]）或支持（例如[10,49,98],) 正式製裁的作用表明，如果不考慮員工的（不可）威懾性，情況仍然模糊，我們的結果支持這樣的斷言，即正式製裁對不情願的遵從者很重要，但對有傾向的遵從者則不重要。同樣，我們的研究還表明，除了正式製裁之外，非正式製裁（例如社會不贊成）會影響不願遵從者而非傾向遵從者的合規決策。傾向遵從者的行為似乎受到一種非正式約束形式的限制，而不是害怕外部製裁，包括正式和非正式（社會）制裁。因此，我們的結果不僅支持這樣的論點，即個人自我制裁作為個人規範的一部分可能具有與一般正式製裁相同的影響 [31]，但甚至足以確保傾斜員工的合規性。

有了這些發現，我們擴展了文獻，表明正式和非正式製裁對合規的有效性取決於一個人的（不）傾向；從而為以後的研究奠定基礎。例如，傾向於員工的數量可能是確定某項政策是否被一部分員工接受的良好指標。在這種情況下，網絡外部性 [99] 可以申請，有意願的員工可以影響那些不願遵守的員工。進一步的研究可以檢查傾向於順從者對他們的同齡人的影響。

如果將兩個合規組（傾向於和不傾向於）視為一個單一的同質組，則這些差異還突出了潛在的錯誤。這些差異在匯總數據中可能並不明顯，在匯總數據中，制裁對政策合規的平均影響可能更多地造成混淆，而不是提供有關威懾過程和製裁鼓勵合規行為的能力的見解。涉及“一刀切”心態的研究並未考慮員工偏好；探索為營造積極態度或專注於製裁言論而量身定制的安全培訓計劃如何說服不同的 員工群體遵守規定將會很有趣。

我們還通過將信息安全政策意識與製裁聯繫起來，研究了傾向於和不傾向於遵守制裁對合規性的威懾作用之外的差異。一些研究表明，政策依賴於與社會法律相同的威懾機制，並且對此的認識會增加正式製裁的看法[52]. 然而，在信息安全研究中幾乎沒有探討信息安全政策意識對非正式（社會）制裁和個人自我制裁的影響。我們表明，基於群體的差異在一定程度上影響信息安全政策意識對多層次製裁的感知（除了懲罰嚴重程度和主觀規範預期之外）。員工似乎對信息安全政策中傳遞的信息的接受程度不同。這些政策既可以作為一種威懾機制來增加外部製裁的認知，也可以作為一種責任機制來形成內部的道德義務感。因此，我們鼓勵進一步研究以利用我們的發現並檢查態度以外的其他因素，這些因素會加劇這兩種機制的差異。

6.3. 實際影響

作為使組織信息安全策略更有效的一種手段，對可阻止性的考慮很重要。由於這些類似於社會法律的政策是基於這樣一種想法，即潛在的政策違反者會受到懲罰威脅的威懾，信息安全經理需要了解這種方法的局限性 [5個]. 基於威懾的信息安全政策和安全教育培訓和意識 (SETA) 計劃應對這種上升的現像只能在員工可威懾的範圍內有效。由於處理業務管理的 IT 和未經批准的雲解決方案已成為安全經理面臨的主要挑戰 [25]，他們需要學習新的策略來教育員工並提高他們的信息安全政策意識。我們的研究承認，提高員工的信息安全政策意識是激勵員工遵守法規的第一步。然而，在設計這些政策和培訓員工以提高他們的意識時，從業者需要注意他們的員工是否更容易接受威懾信息或責任感信息。關鍵的含義是，為提高信息安全策略合規性而採取的行動應注意員工傾向於或不願遵守的不同方式。

例如，旨在通過正式製裁解決威懾問題的舉措，例如宣布員工的計算機活動可能受到監控以及他們將因使用公共雲而受到懲罰，對於對安全政策持積極態度的員工來說很可能仍然無效，因為他們不會被懲罰嚇倒。紀律處分可能對組織有害且代價高昂。首先，如果只有一些員工覺得這些舉措解決了問題，就會浪費組織資源 [4個]. 其次，在某些情況下，實施強制性安全政策變更甚至可能成為消極態度和不良行為的觸發事件或催化劑 [100]. 如果員工出於內在動機而努力遵守政策，制裁威脅可能會降低他們對政策的積極態度。這種通過外部獎勵或懲罰來“排擠”內在行為的現像已被無數行為證實。

領域，例如稅務合規[101]. 相反，我們關於對信息安全政策持積極態度的員工的個人規範與信息安全政策遵守之間關係強度的研究結果表明了一種不同的方法。它們表明具體措施應支持個人規範與信息安全政策的一致性（並克服政策與個人規範之間的差異）。因此，建議組織在信息安全策略的目標和員工的內部價值觀之間形成緊密聯繫，以促進合規性傾向。定期的 SETA 計劃應該努力讓員工認識到信息安全政策的禁令和要求的必要性和有用性。這裡的關鍵點是讓員工相信，保護機密數據也符合他們的最大利益。需要證明數據保護對組織存在的重要性，因此需要證明他們的工作安全，同時表明這些政策也有助於保護員工的個人數據。此外，組織可以訴諸道德培訓來提高員工的道德水平，使他們覺得在道德上有義務遵守信息安全政策。這些道德運動在減少非法行為方面的成功也得到了犯罪學研究的支持 [同時表明這些政策也有助於保護員工的個人數據。此外，組織可以訴諸道德培訓來提高員工的道德水平，使他們覺得在道德上有義務遵守信息安全政策。這些道德運動在減少非法行為方面的成功也得到了犯罪學研究的支持 [同時表明這些政策也有助於保護員工的個人數據。此外，組織可以訴諸道德培訓來提高員工的道德水平，使他們覺得在道德上有義務遵守信息安全政策。這些道德運動在減少非法行為方面的成功也得到了犯罪學研究的支持 [31].

然而，當員工持消極態度時，旨在通過正式或非正式製裁解決威懾問題的 SETA 計劃將促進那些不願遵守信息安全政策的人遵守信息安全政策。我們的研究結果表明，通過懲罰的嚴重程度而不是懲罰的確定性來槓桿化的正式製裁可能更適合對信息安全政策持消極態度的員工。為了鼓勵這些員工的合規行為，信息安全政策的內容應該明確規定對違反安全政策行為的處罰。此外，我們的結果還表明非正式社會制裁的重大影響。上司和同事的期望，當員工對信息安全政策持消極態度時，以及後者的感知行為在影響一個人的安全相關行為方面起著比正式製裁更重要的作用。因此，合規性不應僅通過正式製裁自上而下地強制執行，而應由各級員工（包括主管和 IT 部門）以日常為榜樣。可以對員工的榜樣進行培訓和教育，以提倡合規行為 [102]. 鑑於描述性規範的強大作用，這提出了一個有趣的問題，即警告破壞性安全相關行為增加的信息安全活動（非）有效性（例如，選擇弱密碼和在工作中瀏覽私人網站）提高對安全問題和威脅的認識。通過這樣做，他們傳播了這些行為很普遍的信息。通過傳達“你的許多同事做了不受歡迎的事情”的信息，組織同時傳達了“許多同事正在這樣做”的強烈規範信息[59].

6.4. 局限性和未來的研究

我們研究的以下局限性可以在未來的研究中得到解決。首先，我們的研究可能由於自我報告的合規性而受到限制，因為我們無法觀察到信息安全政策是否符合客觀數據，而是詢問參與者他們是否遵守使用公共雲的組織政策。我們鼓勵研究人員分析組織中實際的公共雲使用情況。然而，組織通常不願意向研究人員披露這些信息，這是現有信息安全研究中經常討論的一個難題 [103]. 儘管如此，通過案例研究解決這個問題將有助於以更豐富的方式驗證和建立我們的發現。

其次，關於態度的概念觀點，我們關注態度效價（即態度的積極或消極性質）。然而，關於縱向設置，我們承認

態度品質或態度強度的概念[104,105] 可能特別重要，尤其是當威懾程度隨時間變化時，因為更強的態度更能抵抗態度改變 [106]. 通過在具有不同威懾程度的縱向設置中引入態度強度的概念，我們很清楚所識別的群體特徵在威懾能力方面可能會有所不同。

第三，我們承認基於對信息安全政策的態度的（不）傾向於遵守的程度可能不是靜態的，而是可能隨著所考慮的安全政策而改變。例如，員工可能喜歡密碼保護政策，因為它有助於保護他們的帳戶，但可能會對雲使用政策感到沮喪，因為它限制了他們共享文件的能力。因此，可能不需要阻止他們與他人共享密碼，但可能需要阻止他們使用公共雲系統。這表明態度和製裁威脅反應之間存在動態緊張關係，未來的研究可以調查這種緊張關係，以評估可遏制性的個體內部一致性程度 [107].

第四，關於方法的局限性，（不）傾向的遵從者的分類是基於對信息安全政策態度的單項測量。尋求擴展和完善此分類的未來研究也可能考慮其他變量，例如習慣，作為（不）傾向於遵守或不遵守的代表。當安全習慣和態度對應時，它們可能導致相同的行為結果，但當它們不對應時，行為結果可能取決於習慣和/或態度的強度。可以確定其他習慣驅動的員工群體來檢查可威懾性，因為當合規行為不是習慣性的但需要思考過程並且是有意的時，制裁的威懾效果可能更有效 [108]. 最後，鑑於我們關注這些（不）傾向於遵守的不同群體的驅動因素和態度，我們還鼓勵研究人員檢查其他不同的群體，例如未能遵守信息安全的具有積極態度的個人政策（“傾向於不遵守者”）和持消極態度因而不遵守的個人（“不遵守者”）。

七、結論

我們對可阻止性的調查很重要，不僅是為了對信息安全政策遵守行為和威懾理論的理論理解，也是使信息安全政策更加有效的一種手段。由於類似於社會法律的信息安全政策是基於這樣一種想法，即潛在的政策違反者會受到懲罰威脅的威懾 [52]，學者和實踐者需要了解這種方法的局限性。通過比較傾向於和不傾向於的遵從者，我們發現多級制裁的威懾效果在對信息安全政策持積極態度和消極態度的員工之間存在差異。我們關於傾向遵從者的調查結果指出了另一條途徑，其中信息安全政策不僅作為一種試圖改變正式製裁觀念的威懾機制，而且作為員工基於個人責任感有義務遵守的事項。此外，提供對先前與威懾相關的信息安全研究的不一致結果的洞察，

CRediT 作者貢獻聲明

倫納特耶格：概念化、方法論、驗證、形式分析、數據規約、寫作原稿、寫作評論 &編輯，可視化。**安德烈亞斯・埃克哈特：**概念化，寫作 - 原稿，寫作 - 評論和編輯，監督。**朱莉婭・克羅農：**概念化、調查、寫作 - 評論和編輯。

附錄 A. 測量不變性

為了評估測量不變性，我們遵循複合模型（MICOM）評估程序的測量不變性，該程序涉及三個步驟[92]. 在第一步中，我們通過確保測量和結構模型的相同設置以及 SmartPLS 中模型估計的相同數據處理和算法設置來建立配置不變性。對於第二步和第三步，我們使用SmartPLS的置換算法。第二步的結果確保了成分不變性（見表 A1) 因為沒有相關性*C*值與一個顯著不同。第三步的結果不支持完全的測量不變性，因為組間的均值和方差不相等。還沒有

表 A1
MICOM 結果。

合成的	***C*值 （¼1)**	**CI95%**	**第 2 步。組合不變性？**
描述性規範	1.000	[0.997; 1.000]	是的
信息安全政策意識 信息安全政策合規性 個	0.948	[0.884; 1.000]	是的
人規範	1.000	[1.000；1.000]	是的
	0.999	[0.998; 1.000]	是的
處罰確定性	0.983	[0.965; 1.000]	是的
處罰力度	0.998	[0.946; 1.000]	是的
主觀規範	0.990	[0.988; 1.000]	是的
合成的	**均值差（¼0)** 0.633	**CI95%**	**步驟 3a。均值相等？** 不
描述性規範		[-0.218; 0.218]	
信息安全政策意識 信息安全政策合規性 個	0.350	[-0.224; 0.243]	不
人規範	1.132	[-0.233; 0.234]	不
	0.967	[-0.226; 0.237]	不
處罰確定性	0.244	[-0.240; 0.227]	不
處罰力度	0.278	[-0.232; 0.249]	不
主觀規範	0.479	[-0.251; 0.198]	不
合成的	**方差對數比 (¼0)** 0.198	**CI95%**	**步驟 3b。方差相等？** 是的
描述性規範		[-0.256; 0.254]	
信息安全政策意識 信息安全政策合規性 個	− 0.064	[-0.334; 0.360]	是的
人規範	− 0.629	[-0.218; 0.234]	不
	− 0.681	[-0.233; 0.202]	不
處罰確定性	0.054	[-0.269; 0.266]	是的
處罰力度	− 0.188	[-0.267; 0.266]	是的
主觀規範	− 0.281	[-0.277; 0.292]	不

比較組間的路徑係數，部分測量不變性就足夠了[92].

附錄 B. 內生性評估

為了評估潛在的內生性，我們遵循 Hult 等人的 [93] 解決 PLS-SEM 中內生性問題的程序，使用高斯 copula 方法 [109]. 這種方法通過聯結函數直接模擬內生變量和誤差項之間的相關性來控制內生性。93]. 我們認為原始模型的自變量以及它們與信息安全政策態度的交互項可能表現出內生性（參見 Papies 等人 [110] 關於高斯 copula 方法中的交互項）。我們使用原始 PLS 模型估計的潛在變量分數作為輸入來計算結構模型中偏回歸的高斯 copula [93]. 為了運行分析，我們使用了 R 程序的 REndo 包 [111]、引導包[112]，以及 Hult 等人提供的 R 代碼。[93]. 我們發現這兩個高斯 copula 都不重要。具體來說，我們發現態度的 0.07 的非顯著聯結 (p-value = 0.52), 0.07 用於描述性規範 (p-value = 0.81), -0.125 信息安全策略意識 (p-value = 0.76), 0.02 為個人規範 (p-value = 0.61)，懲罰確定性為 0.16 (p-value = 0.61), 0.10 表示懲罰嚴重程度 (p-value = 0.65)，主觀標準為 -0.02 (p-值 = 0.56）。此外，將交互項視為潛在內生的，對於態度與描述性規範的交互項，會產生 0.09 的非顯著聯結（p-value = 0.58), 0.11 信息安全策略意識 (p-value = 0.76), 個人標準為 0.035 (p-value = 0.035), -0.11 懲罰確定性 (p-value = 0.64), -0.19 懲罰嚴重程度 (p-value = 0.44)，主觀規範為 0.13 (p-值 = 0.35）。因此，我們得出結論，不存在內生性，這支持了結構模型結果的穩健性 [93].

附錄 C. 補充數據

可以在 doi 的在線版本中找到與本文相關的補充材料：https://doi.org/10.1016/j.im.2020.103318.

參考

[1]R. Willison, M. Warkentin，超越威懾：員工計算機濫用的擴展視圖，MIS Q. 37 (2013) 1-20.
[2]B. Bulgurcu、H. Cavusoglu、I. Benbasat，信息安全政策合規性：基於理性的信念和信息安全意識的實證研究，MIS Q. 34 (2010) 523–548.

[3]DW Straub、RJ Welke，應對系統風險：管理決策制定的安全規劃模型，MIS Q. 22 (1998) 441–469.
[4]AC Johnston、M. Warkentin、AR Dennis、M. Siponen，說他們的語言：設計有效的消息以改進員工的信息安全決策，Decis。科學。50 (2019) 245–284.

[5]M. Silic、JB Barlow、A. Back，中和和威懾的新視角：預測影子 IT 使用情況，Inf。管理。54 (2017) 1023–1037.
[6] KPMG Oracle、Oracle 和 KPMG 雲威脅報告 2019，2019（2019 年 9 月 10 日訪問），https://www.oracle.com/cloud/cloud-threat-report/.
[7] KPMG Harvey Nash，《2019 年 CIO 調查：不斷變化的視角》，2019 年（9 月 10 日訪問，https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/07/ha rvey-nash-kpmg-cio-survey-2019.PDF.
[8] McAfee，在多雲的天空中航行：實用指南和雲安全狀況，2018 年（2019 年 8 月 29 日訪問，https://www.mcafee.com/enterprise/en-us/solutions/lp/cloud-security-report.html.
[9] McAfee，2019 年雲採用和風險報告，2019 年（2019 年 8 月 29 日訪問），https://info.skyhighnetworks.com/WPCloudAdoptionRiskReport2019_Banne rCloud-MFE.html.
[10]JS-C。許，S.-P。Shih、YW Hung、PB Lowry，角色外行為和社會控制在信息安全政策有效性中的作用，Inf。系統。水庫。26 (2015) 282–300.

[11]M. Warkentin, R. Willison，信息系統安全中的行為和政策問題：內部威脅，Eur。J. Inf。系統。18 (2009) 101–105.
[12]J. D'Arcy, T. Herath，IS 安全文獻中威懾理論的回顧和分析：理解不同的發現，Eur。J. Inf。系統。20 (2011) 643–658.

[13]BA Jacobs，威懾和可威懾性，犯罪學 48 (2010) 417–441.

[14]G. Pogarsky，識別“可威懾的”罪犯：對威懾研究的影響，Justice Q. 19 (2002) 431–452.
[15]F. Zimring、G. Hawkins，威懾和邊緣群體，J. Res。犯罪失職。5 (1968) 100–114.

[16]DS Nagin, G. Pogarsky，威懾的實驗研究：作弊、自利偏見和衝動，犯罪學 41 (2003) 167–194.
[17]G. Pogarsky，TA Loughran，威懾中的政策與感知的聯繫：是時候取消清除率了，Criminol。公共政策 15 (2016) 777–790.
[18]DS Nagin, G. Pogarsky，將敏捷、衝動和法外制裁威脅整合到一般威懾模型中：理論和證據，犯罪學 39 (2001) 865–892.

[19]H. Li、XR Luo、J. Zhang、R. Sarthy，工作中互聯網濫用行為的自我控制、組織背景和理性選擇，Inf。管理。55 (3) (2018) 358–367.
[20]V. Braithwaite，與稅務機關共舞：動機姿態和不合規行為，載於：V. Braithwaite（主編），徵稅民主：了解避稅和逃稅，Aldershot，Ashgate，2003 年，第 15-39 頁.

[21]D. McBarnet，當合規不是解決方案而是問題時：從法律的變化到態度的變化，載於：V. Braithwaite（主編），徵稅民主：理解避稅和逃稅，Ashgate，Aldershot，2003 年，第 229-244 頁.
[22] Tom Macaulay，如何確保云中的 GDPR 合規性，2018 年。http://www.computerworlduk.com/cloud-computing/how-ensure-gdpr - 合規性雲 3663797/.
[23] BSI，公共部門的信息和網絡挑戰：2018 年調查，2018 年（2019 年 9 月 10 日訪問），https://www.bsigroup.com/globalassets/localfiles/en-ie/csir/resources/whitepaper/uk-engb-survey-wp-challenges-public-secto r-cloud.pdf.

[24] J. Cook，力挽狂瀾：公共部門如何贏得與影子 IT 的戰鬥，2017 年。https://www.publictechnology.net/articles/opinion/turningtide-how-public-sector-can-win-battle-against-shadow-it.
[25] CIO，公共部門 CIO 應該如何應對“影子 IT”，2015 年。https://www. cio.com.au/article/566649/what-should-public-sector-cios-do-about-shadow-it/.
[26]MR Geerken，WR Gove，威懾：一些理論考慮，Law Soc。修訂版 9 (1975) 497–513.

[27]ML Erickson，JP Gibbs，GF Jensen，威懾學說和法律懲罰的感知確定性，Am。社會學。牧師 (1977) 305–317.
[28]KR Williams, R. Hawkins，關於一般威懾的感知研究：批判性評論，Law Soc。牧師 (1986) 545–572.
[29]JP Gibbs，《犯罪、懲罰和威懾》，Elsevier，紐約，1975 年.
[30]TC Pratt、FT Cullen、KR Blevins、LE Daigle、TD Madensen，威懾理論的實證地位：元分析，載於：FT Cullen、J. Wright、K. Blevins（編），盤點：威懾理論的地位犯罪學理論，交易
出版社，新不倫瑞克，2006 年，第 367–396 頁.
[31]R. Paternoster、S. Simpson，制裁威脅和道德訴求：檢驗企業犯罪的理性選擇模型，Law Soc。修訂版 30 (1996) 549–583.
[32]AR Piquero、R. Paternoster、G. Pogarsky、T. Loughran，闡述威懾理論中的個體差異成分，Annu。法律協會牧師 科學。7 (2011) 335–360.

[33]KH Guo、Y. Yuan、NP Archer、CE Con nelly，了解工作場所的非惡意安全違規行為：複合行為模型，J. Manag。信息。系統。28 (2011) 203–236.

[34]AH Eagly, S. Chaiken, 態度心理學, Harcourt Brace Jovanovich, College Publishers, Fort Worth, TX, 1993.
[35]P. Zhang, SN Aikman, H. Sun, ICT 接受和使用中的兩種態度，Int。J. Hum.-Compu。詮釋。24 (2008) 628–648.
[36]P. Zhang、H. Sun，初始和持續使用 ICT 時不同類型態度的複雜性，J. Assoc。信息。科學。技術。60 (2009) 2048–2063.
[37]N. Sohrabi Safa、R. von Solms、S. Furnell，組織中的信息安全策略合規模型，Comput。安全。56 (2016) 70–82.
[38]HC Kelman，合規、認同和內化：態度改變的三個過程，J. Confl，Resolut。2 (1958) 51–60.
[39]H.-R. Kim, M. Lee, H.-T. 李，N.-M。Kim，企業社會責任和員工-公司身份識別，J. Bus。道德 95 (2010) 557–569.
[40]CM Tam、IWH Fung IV、APC Chan，實施新安全管理體係後人們態度變化的研究：監督計劃，構建。管理。經濟。19 (2001) 393–403.

[41]J. Kroenung、A. Eckhardt、T. Kuhlenkasper，衝突的行為範式和預測 IS 的採用和不採用——基於群體的分析的重要性，Comput。哼。行為。67 (2017) 10–22.

[42]R. Titah，H. Barki，信息技術接受度中態度與主觀規範之間的非線性：負協同作用？MIS Q. 33 (2009) 827–844.

[43]M. Deutsch，HB Gerard，規範和信息社會對個人判斷影響的研究，J. Abnorm。心理學家。51 (1955) 629–636.
[44]Y. Chen, K. Ramamurthy, K.-W. 文，組織的信息安全策略合規性：大棒還是胡蘿蔔？J.馬納格。信息。系統。29 (2014) 157–188.
[45]Y. Xue、H. Liang、L. Wu，強制性 IT 設置中的懲罰、正義和合規性，Inf。系統。水庫。22 (2011) 400–414.
[46]AJ Burns、TL Roberts、C. Posey、RJ Bennett、JF Courtney，合規意圖與保護意圖：理解內部人員對組織 SETA 努力的認識影響的 VIE 理論方法*，Decis。科學。50 (2017) 179–221.

[47]P. Puhakainen、M. Siponen，通過信息系統安全培訓提高員工的合規性：一項行動研究，MIS Q. 34 (2010) 757–778.

[48] S. Matteson，為什麼您的公司需要明確的安全政策：一個警世故事，2017 年。https://www.techrepublic.com/article/why-your-company-needs-cle ar-security-policies-a-cautionary-tale/.
[49]J. D'Arcy、S. Devaraj，員工濫用信息技術資源：測試當代威懾模型，Decis。科學。43 (2012) 1091–1124.
[50]Q. Hu、Z. Xu、T. Dinev、H. Ling，威懾是否有助於減少員工濫用信息安全政策？公社。ACM 54 (2011) 54–60.
[51]DW Straub，有效的 IS 安全性：實證研究，Inf。系統。水庫。1 (1990) 255–276.

[52]J. D'Arcy、A. Hovav、D. Galletta，用戶對安全對策的認識及其對信息系統濫用的影響：一種威懾方法，Inf。系統。水庫。20 (2009) 79–98.
[53]M. Siponen, A. Vance，中和：對員工信息系統安全策略違規問題的新見解，MIS Q. 34 (2010) 487-502.
[54]RE Mann、RG Smart、G. Stoduto、EM Adlaf、E. Vingilis、D. Beirness、R. Lamble、M. Asbridge，酒後駕駛法的影響：差異威懾假說的檢驗，成癮 98 (2003) 1531-1536.
[55]WJ Scott，威懾和所得稅欺詐：測試功利主義理論中的交互假設，J. Appl。行為。科學。17 (1981) 395–408.
[56]M. Wenzel，稅收合規規範流程分析，J. Econ。心理學家。25 (2004) 213–228.

[57]HG Grasmick、RJ Bursik Jr.、良心、重要他人和理性選擇：擴展威懾模型，Law Soc。修訂版 24 (1990) 837–861.
[58]T. Herath、HR Rao，保護動機和威懾：組織中安全策略合規性的框架，Eur。J. Inf。系統。18 (2009) 106–125.
[59]RB Cialdini，描述性社會規範作為社會控制的低估來源，Psychometrika 72 (2007) 263–268.
[60]M. Hartmann、L. Jaeger、A. Eckhardt，幫我一個忙：社會關係對信息安全角色內外行為的作用，載於：第 39 屆信息系統國際會議論文集，加利福尼亞州舊金山， 2018.

[61]V. Venkatesh，FD Davis，技術接受模型的理論擴展：四個縱向實地研究，Manag。科學。46 (2000) 186–204.
[62]PR Warshaw，預測行為意圖的新模型：Fishbein 的替代方案，J. Mark。水庫。17 (1980) 153–172.
[63]SH Schwartz，規範對利他主義的影響，Adv。Exp。社會。心理學家。10 (1977) 221–279.
[64]HG Grasmick、BS Blackwell、RJ Bursik Jr，感知到的製裁威脅的性別模式的變化，Law Soc。修訂版 27 (1993) 679–705.
[65]H. Li, J. Zhang, R. Sarathy，從理性選擇理論的角度理解對互聯網使用政策的遵守，決定。支持系統。48 (2010) 635–645.

[66]P. Ifinedo，信息系統安全政策合規性：社會化、影響和認知影響的實證研究，Inf。管理。51 (2014) 69–79.
[67]IMY Woon, A. Kankanhalli，調查 IS 專業人員實施應用程序安全開發的意圖，Int。J. Hum.-計算機。聖 65 (2007) 29–41.

[68]MT Siponen，組織信息安全意識的概念基礎，Inform。管理。電腦。安全。8 (2000) 31–41.
[69]A. Hovav, J. D'Arcy，應用跨文化威懾的擴展模型：對美國和韓國信息系統濫用的調查，Inf。管理。49 (2012) 99–110.

[70]Q. Hu、T. Dinev、P. Hart、D. Cooke，管理員工遵守信息安全政策：最高管理層和組織文化的關鍵作用，Decis。科學。43 (2012) 615–660.

[71]A. Yazdanmehr，J. Wang，員工信息安全政策合規性：規範激活視角，Decis。支持系統。92 (2016) 36–46.
[72]HLA Hart，責任與報應，牛津大學出版社，牛津，1968 年.

[73]SH Schwartz，JA Howard，責任拒絕對個人規範行為關係的調節作用的解釋，Soc。心理學家。問題 43 (1980) 441–446.

[74]F. Zahedi、A. Abbasi、Y. Chen，假冒網站檢測工具：識別促進個人使用和提高績效的元素，J. Assoc。信息。系統。16 (2015) 448–484.
[75]經過。Ng, A. Kankanhalli, YC Xu，研究用戶的計算機安全行為：健康信念視角，Decis。支持系統。46 (2009) 815–825.
[76]J.-Y。兒子，出於恐懼還是慾望？為了更好地了解員工遵循 IS 安全策略的動機，Inf。管理。48 (2011) 296–302.
[77]M. Siponen、MA Mahmood、S. Pahnila，員工遵守信息安全政策：一項探索性實地研究，Inf。管理。51 (2014) 217 –224.
[78]L. Bergkvist，JR Rossiter，相同結構的多項與單項措施的預測有效性，J. Mark。水庫。44 (2007) 175–184.
[79]WW Chin，結構方程建模的偏最小二乘法，載於：GA Marcoulides（編），現代商業研究方法，Lawrence Erlbaum Associates，Mahwah，新澤西州，1998 年，第 295-336 頁.
[80]J. Henseler，PLS-MGA：基於偏最小二乘法的多組分析的非參數方法，載於：WA Gaul、A. Geyer-Schulz、L. Schmidt-Thieme，J. Kunze（編輯），數據分析、計算機科學和優化接口的挑戰，施普林格，卡爾斯魯厄，2012 年，第 495-501 頁.
[81]JF Hair、WC Black、BJ Babin、RE Anderson、RL Tatham，多變量數據分析，Pearson Prentice Hall Upper Saddle River，新澤西州，2006 年.
[82]J. Hulland，在戰略管理研究中使用偏最小二乘法 (PLS)：對最近四項研究的回顧，Strat。管理。雜誌 20 (1999) 195–204.
[83]C. Fornell，DF Larcker，用不可觀測變量和測量誤差評估結構方程模型，J. Mark。水庫。18 (1981) 39–50.

[84]J. Henseler、CM Ringle、M. Sarstedt，基於方差的結構方程模型中判別有效性評估的新標準，J. Acad。標記。科學。43 (2015) 115–135.

[85]AH Gold、A. Malhotra、AH Segars，知識管理：組織能力視角，J. Manag。信息。系統。18 (2001) 185–214.
[86]MK Lindell，DJ Whitney，橫斷面研究設計中常見方法差異的解釋，J. Appl。心理學家。86 (2001) 114–121.
[87]NK Malhotra、SS Kim、A. Patil，IS 研究中的通用方法差異：替代方法的比較和對過去研究的重新分析，Manag。科學。52 (2006) 1865–1883.

[88]R. Agarwal, E. Karahanna，當你玩得開心時，時光飛逝：認知吸收和對信息技術使用的信念，MIS Q. 24 (2000) 665–694.

[89]L. Matthews，在 PLS-SEM 中應用多組分析：一個循序漸進的過程，在：H. Latan, R. Noonan（編輯），偏最小二乘路徑建模：基本概念、方法論問題和應用，Springer International Publishing，Cham，2017 年，第 219-243 頁.

[90]JF Hair Jr.，GTM Hult，C. Ringle，M. Sarstedt，偏最小二乘結構方程建模 (PLS-SEM) 入門，SAGE 出版物，2016 年.
[91]C. Schlaegel，M. Sarstedt，評估跨國家四維文化智力量表的測量不變性：複合模型方法，Eur。管理。J. 34 (2016) 633–649.

[92]J. Henseler、CM Ringle、M. Sarstedt，使用偏最小二乘法測試複合材料的測量不變性，Int。標記。修訂版 33 (2016) 405–431.
[93]GTM Hult、JF Hair Jr、D. Proksch、M. Sarstedt、A. Pinkwart、CM Ringle，解決偏最小二乘結構方程模型國際營銷應用中的內生性問題，J. Int。標記。26 (2018) 1–21.

[94]CR Tittle, R. Paternoster, 社會偏差和犯罪：一種組織和理論方法，羅克斯伯里出版公司，加利福尼亞州洛杉磯，2000 年.
[95]L. Ross、D. Greene、P. House，“虛假共識效應”：社會認知和歸因過程中的自我中心偏見，J. Exp。社會。心理學家。13 (1977) 279–301.

[96]PB Lowry、C. Posey、RBJ Bennett、TL Roberts，利用公平和反抗理論來阻止遵循增強的組織信息安全策略的反應性計算機濫用：反事實推理和組織信任影響的實證研究，信息。系統雜誌 25 (2015) 193–273.

[97]M. Warkentin、AC Johnston、J. Shropshire，非正式社會學習環境對信息隱私政策合規效力和意圖的影響，Eur。J. Inf。系統。20 (2011) 267–284.

[98]AC Johnston, M. Warkentin, MT Siponen, 增強的恐懼訴求修辭框架：通過制裁修辭利用對人類資產的威脅，MIS Q. 39 (2015) 113–134.
[99]D. Katz，組織行為的動機基礎，Syst。水庫。9 (1964) 131–146.

[100]F. Bélanger、S. Collignon、K. Enget、E. Negangard，早期遵守信息安全政策的決定因素，Inf。管理。54 (2017) 887–901.
[101]LP Feld，BS Frey，心理稅收契約導致的稅收合規：激勵和響應監管的作用，Law Policy 29 (2007) 102-120.
[102]L． 2017年.

[103]RE Crossler、AC Johnston、PB Lowry、Q. Hu、M. Warkentin、R. Baskerville，行為信息安全研究的未來方向，Comput。安全。32 (2013) 90–101.

[104]JA Krosnick，RE Petty，態度強度：前因後果，心理學出版社，紐約，1995 年.

[105]MW Erber、SD Hodges、TD Wilson，態度強度、態度穩定性和分析原因的影響，載於：RE Petty、JA Krosnick（編）、編），態度強度：前因後果，心理學出版社，紐約，1995，第 433–454 頁.
[106]EM Pomerantz、S. Chaiken、RS Tordesillas，態度強度和阻力過程，J. Pers，Soc。心理學家。69 (1995) 408–419.
[107]JA Bouffard、ML Exum、N. Niebuhr，檢查定罪重罪犯樣本中多種犯罪類型的穩定性和可遏制性預測因素，J.克里姆。正義 57 (2018) 76–88.
[108]D. Beyleved，識別、解釋和預測威懾，Br。J.犯罪。19 (1979) 205–224.

[109]S. Park、S. Gupta，通過使用 copula 的聯合估計處理內生回歸變量，Mark。科學。31 (2012) 567–586.
[110]D. Papies、P. Ebbes、HJ van Heerde，解決營銷模型中的內生性問題。市場建模的高級方法，Springer，2017 年，第 581-627 頁.
[111] R. Gui、M. Meierer、R. Algesheimer、R. Package REndo，使用潛在工具變量擬合具有內生回歸變量的線性模型（1.2 版），2017 年。 https://cran.r-project.org/web/packages/REndo/.
[112] A. Canty，B. Ripley，R Package Boot：Bootstrap Functions（版本 1.3-20），2017（2019 年 8 月 29 日訪問，https://cran.r-project.org/web/packages/boot/.

倫納特耶格是德國 Oestrich-Winkel 的 EBS 商業與法律大學的助理研究員。他畢業於法蘭克福歌德大學信息系統專業。他的研究興趣包括信息安全的行為和組織方面。他的研究已發表在多個 IS 會議的論文集中，例如 ICIS、ECIS、PACIS 和 HICSS。他獲得了 ECIS 2018 和 SIGADIT 頒發的最佳論文獎。

安德烈亞斯・埃克哈特是位於海爾布隆的德國管理與法律研究生院 (GGS) 的教授，也是因斯布魯克大學信息系統的客座教授。他獲得了博士學位。法蘭克福歌德大學信息系統專業。他在 IT 採用和用戶行為、行為安全、數字創新、技術壓力和 E-HRM 方面的研究已發表在兩本書、幾本書章節、會議論文集和科學期刊中，包括信息技術雜誌、戰略信息系統雜誌、歐洲信息系統雜誌、信息與管理、商業與信息系統工程和 MIS 季刊執行官。他因其研究、教學和社區工作而獲得無數獎項，其中包括 Magid Igbaria 傑出論文獎和 ECIS 最佳研究進展論文獎。他是 AIS 特別興趣的前任主席信息技術採用和傳播小組 (SIGADIT)，以及 AIS 多元化和包容性委員會的成員。

朱莉婭・克羅農是德國 Oestrich-Winkel 的 EBS 商業與法律大學的教授。她的研究重點是電子政務、人類行為和信息系統、社會包容和個人信息系統採用。她的研究成果發表在多個科學期刊上，包括信息系統協會期刊、信息與管理、人類行為計算機、信息技術理論與應用期刊、國際電子商務期刊、Cogent Business &管理，以及領先的 IS 會議的會議記錄，例如國際信息系統會議。