She’s worth IT: challenges for female CIOs in ensuring IT security compliance

Gaurav Bansal and Zhuoli Axelton
University of Wisconsin – Green Bay, Green Bay, Wisconsin, USA

Abstract

Purpose – IT security compliance is critical to the organization’s success, and such compliance depends largely on IT leadership. Considering the prevalence of unconscious gender biases and stereotyping at the workplace and growing female leadership in IT, the authors examine how the internalization of stereotype beliefs, in the form of the employee’s gender, impacts the relationships between leadership characteristics and IT security compliance intentions.

Design/methodology/approach – A controlled experiment using eight different vignettes manipulating Chief Information Officer (CIO) gender (male/female), Information Technology (IT) expertise (low/high) and leadership style (transactional/transformational) was designed in Qualtrics. Data were gathered from MTurk workers from all over the US.

Findings – The findings suggest that both CIOs’ and employees’ gender play an important role in how IT leadership characteristics – perceived expertise and leadership style – influence the employees’ intentions and reactance to comply with CIO security recommendations.

Research limitations/implications – This study’s findings enrich the security literature by examining the role of leadership styles on reactance and compliance intentions. They also provide important theoretical implications based on gender stereotype theory alone: First, the glass ceiling effects can be witnessed in how men and women employees demonstrate prejudice against women CIO leaders through their reliance on perceived quadratic CIO IT expertise in forming compliance intentions. Secondly, this study’s findings related to gender role internalization show men and women have a prejudice against gender-incongruent roles wherein women employees are least resistive to transactional male CIOs, and men employees are less inclined to comply with transactional female CIOs. This confirms the findings related to gender internationalization from Hentschel et al. (2019).

Practical implications – This study highlights the significance of organizations and individuals actively promoting gender equality and fostering environments that recognize women’s achievements. It also underscores the importance of educating men and women about the societal implications of stereotyping gender roles that go beyond the organizational setting. This research demonstrates that a continued effort is required to eradicate biases stemming from gender stereotypes and foster social inclusion. Such efforts can positively influence how upcoming IT leaders and employees internalize gender-related factors when shaping their identities.

Social implications – This study shows that more work needs to be done to eliminate gender stereotype biases and promote social inclusion to positively impact how future IT leaders and employees shape their identities through internalization.

Originality/value – This study redefines the concept of “sticky floors” to explain how subordinates can hinder and undermine female leaders, thereby contributing to the glass ceiling effect. In addition, the study elucidates how gender roles shape employees’ responses to different leadership styles through gender stereotyping and internalization.

Keywords CIO gender, Employee gender, IT expertise, Leadership style, IT security compliance, Stereotype, Internalization, Glass ceiling, Sticky floors

Paper type Research paper

1. Introduction

The most recent research in the realm of IT security compliance highlights the crucial role played by cybersecurity initiatives and underscores the importance of comprehending behaviors linked to information security (Cram and D’Arcy, 2023; Frank and Kohn, 2023; Liang...
et al., 2023; Merhi and Ahluwalia, 2023; Yin et al., 2023). Two prevailing notions have gained widespread acceptance in the IT security literature. First, frequent ransomware attacks and unceasing data breaches have invariably pushed information security threats as a major concern for any organizational leadership (Purdy, 2021). Second, it is not the technology but the employees who are the weakest link in the organization’s success in information security compliance (Bansal and Warkentin, 2021; Bulgurcu et al., 2010). It is also established that organizational leadership, particularly IT leadership and the CIO role, is vital in influencing employees’ compliance with security policy (e.g. Guhr et al., 2019). However, due to unconscious biases and stereotyping threats (Buckalew et al., 2012; Eagly et al., 2000) prevalent even today in our society and organizations, a leader’s gender (such as CIO gender) could influence employees’ compliance intentions differently. The stereotyping is not only related to characterizing others but is also associated with how individual men and women internalize and shape their gender identities differently based on how they perceive gender roles are being played out in society (Bem, 1974; Eagly et al., 2020; Hentschel et al., 2019; Wood and Eagly, 2015).

A growing body of scholarship documents the prevalence of unconscious gender biases in modern work organizations (Heilman, 2012). Both survey and experimental studies indicate that men are often believed to be more competent and agentic than women (Koenig and Eagly, 2014). Stereotyping is a serious challenge female business leaders face, especially in IT, as Information Technology has traditionally been male-dominated (Reid et al., 2010). Due to this stereotyping threat, female CIOs are conferred lower social status (McDonald et al., 2004). They must surpass higher benchmarks to attain the same organizational levels as their male counterparts. They are also expected to be more communal and assumed to follow a transformational leadership style, unlike men, who are expected to be more transactional in leadership style (Saint-Michel, 2018; Wang et al., 2013). Moreover, individuals internalize gender roles differently based on their experiences and observations, leading to varying self-perceptions among men and women. Those gender roles are primarily categorized along two dimensions – agentic and communal (Hentschel et al., 2019). Research suggests that due to differences in stereotype internalization, “[m]ale raters generally described women as being less agentic than men and as less agentic than female raters described them” (Hentschel et al., 2019, p. 1). Such different degrees of gender stereotype internalization will shape how male and female employees view and expect how male and female CIOs should act and behave. Little research examines such stereotype and internalization factors in the context of IT security compliance and IT leadership in MIS.

Findings in stereotype literature also suggest that any incongruence in expected gender roles could lead to prejudice (Eagly and Karau, 2002), disapproval and reactance. We argue that in the context of IT security compliance, the CIO’s non-conforming social roles due to stereotyping and gender bias can lead to disapproval and cause reactance among employees to the security compliance recommendations by leaders. Reactance is considered a resistive force that leads people to resist the social influence of others to regain threatened or lost freedom (Lowry and Moody, 2015). This study relies on Johnson and Buboltz (2000)’s definition of reactance as a resistance to persuasion due to one’s need for independence and autonomy, particularly in reaction to a threat to one’s freedom and a tendency to oppose authority. Research suggests that reactance can be aroused not only by direct threats but by those that are subtly and outside of conscious awareness (Miron and Brehm, 2006; Steindl et al., 2015) – such as role incongruence and stereotypes.

In the context of the glass ceiling, which is defined as a barrier of prejudice and discrimination that excludes women from higher-level leadership positions (Eagly and Karau, 2002), it is shown that the odds of success for advancement at higher ranks (e.g. C suites) vary for men and women – with disproportionally higher odds of success for men (Cotter et al., 2001). Thus, using the stereotyping, role congruity theory, reactance and glass ceiling theoretical lenses, we examine the moderating role of CIO gender on the relationship
between perceived IT expertise (as credibility) and leadership style in influencing employees’ intention and reactance to comply with security policy recommendations. In particular, we are interested in examining the quadratic effect of perceived IT expertise, which refers to a nonlinear relationship where compliance intentions strengthen more rapidly as perceived IT expertise grows. We also examine how the internalization of stereotype beliefs, in the form of the employees’ gender, impacts these relationships. The research question was examined using an experimental survey conducted through MTurk. The findings show that gender—both CIOs’ and employees’, plays an important role in how IT leadership characteristics—perceived IT expertise and leadership style influence the employees’ intentions and reactance to comply with CIO security recommendations.

The study has theoretical, social and practical implications. It helps inform IT literature on the role of the security message sender’s characteristics and the contextual outcomes. CIO gender and the role of gender stereotypes in information security compliance and IT literature is an important but relatively understudied area. Even though women’s role in business and IT leadership is growing, there is little research to date to guide women business leaders and CIOs (Dwivedi et al., 2018). Theoretically, our findings enrich stereotype literature by showing how subtle and subconscious gender stereotype beliefs and associated role incongruency could create reactance and lower intentions to comply with CIO security recommendations. The findings show how males and females in our society have internalized gender roles differently and the implications it has for the empowerment of female CIOs. Our study also helps explain the factors that could be associated with the glass ceiling effect, which lowers the career progression of female CIOs. The study highlights that including employee gender is important in understanding gender-based differences in IT leadership. This study provides practical guidance to organizations and individuals on how they can advance gender equality. Our work also has social implications. It creates awareness of the extent of stereotyping and society’s expectations of gender roles still prevalent today while at the same time responding to the calls for increased attention to social inclusion issues in the IT field and gender diversity in IT organizations (Jia et al., 2022).

2. Theoretical foundations and literature review
2.1 Leadership characteristics and compliance behavior
Prior research on CIO leadership characteristics and employee security compliance behavior suggests leadership styles are vital in influencing security compliance behavior (e.g. Feng et al., 2019a; Guhr et al., 2019). Guhr et al. (2019) provide insights into the effects of leadership style on employees’ security compliance behavior using a full-range leadership model. Their study considers a complete range of management leadership behaviors—transformation leadership, transactional leadership and passive/avoidant leadership. It shows that transformational leadership is best suited to achieve the desired compliance intentions in comparison to transactional and passive/avoidant behaviors. In addition, transformational leaders who actively participate in and communicate about security initiatives can positively impact employee attitudes and perceived control over security compliance (Flores and Ekstedt, 2016; Guhr et al., 2019; Hu et al., 2012).

Using the lens of social bond theory, Feng et al. (2019a) show that all three dimensions of paternalistic leadership—benevolence, morality and authoritarianism—positively influence employee information security compliance. Based on social learning theory and information processing theory, Xue et al. (2018) investigate the relationship between ethical leadership and employees’ compliance intentions and the mediation effect of organizational information security climate. Table 1 provides a summary of the extant research in this domain.

Moreover, a strong security culture at the company, fostered by top management’s commitment to security, also promotes employee compliance (D’Arcy and Greene, 2014).
When top management prioritizes security, employees develop positive attitudes and norms around compliance and perceive greater control over compliant behavior (Hu et al., 2012).

2.2 CIO gender – gender bias, stereotype and role congruity theory
The CIO position is largely male-dominated (Dawson et al., 2015), resulting in an unlevel playing field for female CIOs as gender status beliefs shape expectations differently for female leaders on male-typed tasks (Ridgeway, 2011). Gender biases make people systematically undervalue the competence of female business leaders. Thébaud (2015) reports that women managers are often believed to be less achievement-oriented and less competent than their male counterparts, subjecting them to a stricter performance standard. These stereotyping threats require women with similar abilities to work harder than men and face relatively more obstacles (Dryburgh, 1999).

Stereotype literature suggests that men are expected to display agentic characteristics, while women are expected to display communal characteristics and concern for others (Saint-Michel, 2018). Moreover, any incongruence in expected gender roles could lead to prejudice (Eagly and Karau, 2002) and thus increase disapproval and reactance. More specifically, Eagly and Karau (2002) define their role congruence theory as follows – “[a] potential for prejudice exists when social perceivers hold a stereotype about a social group that is incongruent with the attributes that are thought to be required for success in certain classes of social roles” (p. 574).

2.3 Employee’s gender – internalization and shift of gender stereotypes
It is reportedly argued that gender stereotypes characterize others but also oneself (Bem, 1974; Hentschel et al., 2019). Stereotyped characteristics can be internalized and become part of a person’s gender identity (Wood and Eagly, 2015). The internalization process starts in childhood when humans learn to behave in gender-appropriate and stereotype-congruent ways from their immediate environment (Bem, 1974). The internalization of stereotypes happens differently for men and women. Highlighting such differences, Hentschel et al. (2019) report that women tended to characterize themselves in more stereotypic terms (i.e. less assertive and less competent in leadership) than they characterized other women. However, men characterized themselves in less stereotypic terms (i.e. more communal). A more recent study (Tremmel and Wahl, 2023) broadens the insight into prevailing gender stereotypes using the approach of social representations collected through free associations. Their study finds that women evaluate characteristics associated with female leaders more negatively than those associated with typical male leaders.

<table>
<thead>
<tr>
<th>Source</th>
<th>Leadership characteristics</th>
<th>Security compliance intention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feng et al. (2019a)</td>
<td>Paternalistic leadership – benevolence, morality and authoritarianism</td>
<td>Employees’ information security policy (ISP) compliance</td>
</tr>
<tr>
<td>Flores and Ekstedt (2016)</td>
<td>Transformational leadership</td>
<td>Employees’ intention to resist social engineering</td>
</tr>
<tr>
<td>Guhr et al. (2019)</td>
<td>Full-range leadership – transformational leadership, transactional leadership and passive/avoidance leadership</td>
<td>Employees’ in-role and extra-role behavior in the form of information security compliance intention</td>
</tr>
<tr>
<td>Xue et al. (2021)</td>
<td>Ethical leadership</td>
<td>Employees’ information security policy (ISP) violation intention</td>
</tr>
</tbody>
</table>

Table 1. Salient review of literature examining leadership traits and compliance behavior

Source(s): Authors’ creation/work
3. Research model and hypotheses
Our research examines the role of gender and leadership characteristics in impacting the employees’ reactance and intention to comply with the CIO’s security policy recommendations. More specifically, our research focuses on the gender of the leader (CIO) and employee. Figure 1 presents the research model and hypotheses.

3.1 The role of gender on employees’ compliance with CIO security recommendations
3.1.1 Quadratic effect of perceived CIO IT expertise. According to social role theory (Eagly and Wood, 2012; Koenig and Eagly, 2014), gender stereotypes stem from people’s direct and indirect observations of women and men in their social roles. Hence, the presence of very few women in the IT field contributes to the internalization that men are better than women in IT-related skills. Perceived higher expertise of leaders is associated with higher employee approval and lower reactance (Brown and Raven, 1994).

Prior studies investigating the glass ceiling effect suggest that gender disparities tend to be more pronounced at higher organizational levels compared to lower levels. Further, the extent of glass ceiling inequality tends to increase over the course of one’s career (Cotter et al., 2001). Their findings indicate that as individuals advance in their careers, the disparity in performance perceptions and acceptance based on gender intensifies at an increasing rate, suggesting a quadratic effect. Further, this quadratic effect is more pronounced for male leaders than for female leaders.

Considering gender stereotype biases and the glass ceiling effect, we argue that the female CIO’s perceived IT expertise will be discounted systematically, thus leading to lower compliance intentions than her male counterpart. Similarly, the quadratic effect of perceived expertise on lowering the employees’ reactance will be more pronounced for male CIOs than female CIOs.

Moreover, we assert that female employees, driven by heightened self-doubt and an amplified perception of male leaders’ capabilities, especially in IT domains where men in...
leadership positions are perceived to hold an advantage, will contribute to a more pronounced influence of IT expertise on male CIOs. This phenomenon can be attributed to the internalization of gender roles, exacerbated by the underrepresentation of women in STEM fields and reinforces beliefs in male dominance within the technical and IT sectors (Nosek et al., 2009). As a result, male CIOs working with female employees will experience a more evident increase in intention and a decrease in reactance compared to male CIOs with male employees.

Conversely, male employees, driven by similar factors, are more inclined to underestimate female CIOs’ IT expertise than their female counterparts. These beliefs are driven by the mutual reinforcement of gender stereotypes, where female employees view male CIOs as opposed to female CIOs as more capable; male employees view female leaders as less capable and males as more adept IT leaders. Furthermore, this tendency is influenced by males’ greater propensity to adhere to traditional gender stereotypes that favor their gender (Hentschel et al., 2019). Consequently, we argue that the impact of a female CIO’s IT expertise, characterized by an increased intention and reduced reactance, will be less conspicuous among male employees than their female counterparts.

Therefore, we hypothesize that:

**H1a.** The quadratic effect of perceived CIO IT expertise is positively associated with the employees’ intention to comply with the CIO security recommendation, such that (i) the effect is stronger for male CIOs (M) than female CIOs (F) and (ii) the effect is stronger for male CIOs–female employees (MF), as opposed to male CIOs–male employees (MM), and the effect is weaker for female CIOs–male employee (FM), as opposed to female CIOs–female employees (FF).

**H1b.** The quadratic effect of perceived CIO IT expertise is negatively associated with the employees’ reactance to comply with the CIO security recommendation, such that (i) the effect is stronger for male CIOs (M) than female (F) CIOs and (ii) the effect is stronger for male CIOs–female employees (MF), as opposed to male CIOs–male employees (MM), and the effect is weaker for female CIOs–male employee (FM), as opposed to female CIOs–female employees (FF).

### 3.1.2 CIO leadership styles – transformational vs transactional styles.

It is known that female leaders are more transformational than their male counterparts (Eagly et al., 2003). The stereotype and role congruency theory (Eagly and Karau, 2002) suggests that they are also expected to act according to these roles – men are expected to display agentic characteristics, while women are expected to display communal characteristics and concern for others (Saint-Michel, 2018). The same theory also suggests that women are expected to demonstrate communal qualities (and thus a transformational leadership style) more than men, who are expected to be transactional leaders (Tyssen et al., 2014).

The role congruence theory would suggest that a female (male) CIO with a transformational (transactional) leadership style is more likely to generate less reactance and higher compliance behavior among all employees. Thus, we argue that the effect of the transformational (transactional) leadership style on the employees’ compliance with security policy could be stronger for female (male) CIOs.

It is known that unconscious gender biases and stereotyping create reactance effects when people encounter stimuli incongruent with social roles (Miron and Brehm (2006). Having a female CIO with a transactional leadership style or a male CIO with a transformational leadership style could trigger reactance and create disapproval in the form of lower intentions among employees based on their expectations regarding traditional gender roles and leadership styles. Thus, we argue that the effect of the transformational (transactional) leadership style on the employees’ reactance to security recommendations could be stronger for male (female) CIOs.
However, the role incongruence of the CIO leadership style and gender will impact male and female employees differently. Male employees will be more likely to comply with a female CIO with a transformational leadership style than female employees – the reason being men are found to describe themselves as more agentic and women as more communal than female raters described themselves (Hentschel et al., 2019). Similarly, female employees, as opposed to male employees, are more likely to comply with a CIO with a transactional leadership style.

Even though it is known that both leadership styles are effective (Tyssen et al., 2014), incongruent leadership roles might cause reactance. Thus, we argue that female employees are more (less) likely to react to a male CIO with a transformational (transactional) leadership style. Similarly, male employees are more (less) likely to react negatively to a female CIO with a transactional (transformational) leadership style.

Hence, we hypothesize that:

H2a. Transformation leadership style is positively associated with the employees’ intention to comply with the CIO security recommendation, such that (i) the effect is stronger for female CIOs (F) than male CIOs (M) and (ii) the effect is weaker for male CIOs–female employees (MF), as opposed to male CIOs–male employees (MM), and the effect is stronger for female CIOs–male employee (FM), as opposed to female CIOs–female employees (FF).

H2b. Transformation leadership style is positively associated with the employees’ reactance to comply with the CIO security recommendation, such that (i) the effect is stronger for male CIOs (M) than female CIOs (F) and (ii) the effect is stronger for male CIOs–female employees (MF), as opposed to male CIOs–male employees (MM), and the effect is weaker for female CIOs–male employee (FM), as opposed to female CIOs–female employees (FF).

H3a. Transactional leadership style is positively associated with the employees’ intention to comply with the CIO security recommendation, such that (i) the effect is stronger for male CIOs (M) than female CIOs (F) and (ii) the effect is stronger for male CIOs–female employees (MF), as opposed to male CIOs–male employees (MM), and the effect is weaker for female CIOs–male employee (FM), as opposed to female CIOs–female employees (FF).

H3b. Transactional leadership style is positively associated with the employees’ reactance to comply with the CIO security recommendation, such that (i) the effect is stronger for female CIOs (F) than male CIOs (M) and (ii) the effect is weaker for male CIOs–female employees (MF), as opposed to male CIOs–male employees (MM), and the effect is stronger for female CIOs–male employee (FM), as opposed to female CIOs–female employees (FF).

4. Research methodology

4.1 Experiment instrument

A controlled experiment using eight different vignettes manipulating CIO gender (male/female), IT expertise (low/high) and leadership style (transactional/transformational) was designed in Qualtrics. Appendix 1 shows the details of the vignettes used in the experiment. Intention items were adapted from Bansal et al. (2020), reactance items were adapted from Lowry and Moody (2015), perceived IT expertise items were adapted from Bhattachjee and Sanford (2006), leadership style items were adapted from Eberlin and Tatum (2008) and Ismail et al. (2010). We also controlled for AWS (attitude towards women scale) (Spence and Hahn, 1997), threat susceptibility (Johnston et al., 2015), and the linear effect of expertise,
age and perceived victimization. We used two-item scales for AWS leadership style – it is suggested that “a factor with two variables is only considered reliable when the variables are highly correlated with each another (r > 0.70) but fairly uncorrelated with other variables” (Yong and Pearce, 2013, p. 80). The instrument and the source of the items are listed in Appendix 2 and Appendix 3, respectively. Experiment flow is shown in Appendix 4.

4.2 Data collection
The study was conducted online, and data were gathered from subjects solicited through Amazon Mechanical Turk (MTurk). The authors obtained IRB approval from their institution (Protocol#22-Fall-22). All participants provided consent to the study. We restricted the participants’ location to “U.S.” to eliminate any confounding effects due to country of origin. The participants are randomly assigned to one of the eight different scenarios. The demographics of the respondents are shown in Table 2. There were 388 males and 316 females in the final sample. 58.2% indicated that they had previously fallen victim to a phishing attack. Regarding education – 53.4% self-reported a college degree, and 40.5% indicated a master’s degree or higher. After removing incomplete and respondents who failed attention checks, we had seven hundred and four useable responses.

5. Data analysis and results
5.1 Measurement validation and manipulation checks
Several tests were performed to ensure the validity of our measures. First, we assess the construct reliability using Cronbach’s alpha and composite reliability measures for each group and subgroup. We assessed the discriminant and convergent validities of the measures using the Fornell-Larcker criterion. The square roots of the AVE values were generally higher than any of the construct correlations, showing that the measures meet adequate discriminant validity. The square root of AVE values is greater than 0.7 (except for Intentions AVE = 0.60 for the male CIO group and AVE = 0.61 for the female CIO group), showing that the measures meet convergent validity. Second, we performed exploratory factor analysis (EFA) for all the subgroups. The items showed high loadings on their intended constructs (>0.7) and low cross-loadings of individual items to constructs, which suggest high convergent and discriminant validity. Finally, we tested the dataset for the presence of common method variance. The common method variance analyses are reported in Appendix 5. Smart PLS found the second lowest positive correlation to be low and non-significant, which indicates that common method variance is not a major concern in this study.

We check the effectiveness of our manipulation checks – expertise and leadership style. For expertise – we conducted ANOVA for each of the three perceived expertise items (EXP1, EXP2 and EXP3) and found that the mean score for these items was significantly higher (p values of 0.015, 0.003 and 0.002, respectively) for respondents who were shown high expertise condition vignette than those who were shown the low expertise condition vignette –supporting the success of manipulation. For leadership style, we found that TRF2 was

<table>
<thead>
<tr>
<th></th>
<th>CIO male</th>
<th>CIO female</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee male</td>
<td>280 (33.49, 9.11)</td>
<td>175 (34.82, 10.41)</td>
<td>455 (34, 9.64)</td>
</tr>
<tr>
<td>Employee female</td>
<td>108 (36.63, 10.52)</td>
<td>141 (36.94, 10.72)</td>
<td>249 (36.81, 10.61)</td>
</tr>
<tr>
<td>Total</td>
<td>388 (34.36, 9.62)</td>
<td>316 (35.77, 10.58)</td>
<td>704 (35, 10.08)</td>
</tr>
</tbody>
</table>

Table 2. Demographics
Source(s): Author’s creation/work
significantly higher for respondents who were shown the transformation condition vignette than those who were shown the transactional one. The mean scores for TRF1 were higher for the transformational vignette than for the transactional one, and the mean scores for TRC1 and TRC2 were higher for transactional vignettes than for the transformation one – the mean differences were not significant, but the mean scores moved in the expected direction, providing support for our leadership manipulation. We further tested the leadership manipulation using two quiz questions embedded in the survey at the beginning and the end, measuring the leadership style as motivating and punishment-oriented. The one-sample proportion Z-test tested if the respondents identified with the correct style (Quiz1: 81.8% of the respondents identified correctly as transformational, and 66.0% identified correctly as transactional; both were significant at a \( p \)-value of 0.000 each, respectively). The second quiz embedded in the survey also showed similar results – proportion values of 81 and 64.8%, respectively, with \( p \) values of 0.000 each. The results indicated that our experimental manipulation was successful and worked as intended.

5.2 Hypotheses testing

We tested all the hypotheses through partial least squares structural equation modeling (PLS-SEM) using SmartPLS. PLS-SEM was used because it can analyze direct and indirect effects with multi-item constructs and is less restrictive on the sample than covariance-based SEM methods (Ringle et al., 2015). Each model had high \( R \)-square values for compliance intention and reactance, ranging from 0.605 to 0.766. Table 3 reports the \( R \)-square values of different groups and subgroups.

Consistent multigroup bootstrapping analysis (MGA) in SmartPLS was used to contrast the differences between male (M) and female CIOs (F) groups and also the two subgroup combinations (MF and MM; and FM and FF). We also evaluated the M and F groups for structural moderation – where the path is significant in one group and insignificant in the other (Bansal et al., 2015).

Before evaluating the hypotheses, we tested for measurement invariance. All the items demonstrated measurement invariance across Male and Female CIO groups at \( p < 0.05 \) level. All pairwise subgroups also demonstrated measurement invariance, with minor exceptions, wherein MM-MF and FM-FF had two items, each with slightly lower \( p \)-values. Since there were only minor deviations, we decided to keep all the items. Table 4 reports the findings of the comparisons along with the path coefficients and significance values obtained for individual groups and pairwise MGA subgroup comparisons.

5.3 Results

The MGA analysis results (see Table 4) offer support for H1a(i) and H1a(ii), as well as partial support for H1b(ii), but they do not support H1b(i). We observed that the quadratic impact of CIO IT expertise on employees’ intention to comply with CIO security recommendations is

<table>
<thead>
<tr>
<th></th>
<th>M</th>
<th>F</th>
<th>MM</th>
<th>MF</th>
<th>FM</th>
<th>FF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intention</td>
<td>0.726</td>
<td>0.671</td>
<td>0.763</td>
<td>0.756</td>
<td>0.688</td>
<td>0.696</td>
</tr>
<tr>
<td>Reactance</td>
<td>0.620</td>
<td>0.702</td>
<td>0.605</td>
<td>0.686</td>
<td>0.766</td>
<td>0.634</td>
</tr>
</tbody>
</table>

**Note(s):** M: Male CIO; F: Female CIO; MM: Male CIO-Male Employees; MF: Male CIO-Female Employees; FM: Female CIO-Male Employees; FF: Female CIO-Female Employees

**Source(s):** Authors’ creation/work

Table 3. \( R \) square for different groups

Challenges for female CIOs
<table>
<thead>
<tr>
<th>Hyp</th>
<th>Path</th>
<th>CIO/Employee gender</th>
<th>Coef</th>
<th>T-stat</th>
<th>Sig</th>
<th>Coef</th>
<th>T-stat</th>
<th>Sig</th>
<th>Remarks (consistent bootstrapping MGA, two tails)</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1a(i) Expertise2 (\rightarrow) Int</td>
<td>CIO gender</td>
<td>M</td>
<td>0.077</td>
<td>2.936</td>
<td>0.003</td>
<td>F</td>
<td>0.063</td>
<td>1.468</td>
<td>0.143</td>
</tr>
<tr>
<td></td>
<td>CIO (\Sum) Employee gender</td>
<td>MM</td>
<td>0.064</td>
<td>2.043</td>
<td>0.042</td>
<td>FM</td>
<td>0.079</td>
<td>1.243</td>
<td>0.215</td>
</tr>
<tr>
<td></td>
<td>CIO (\Sum) Employee gender</td>
<td>MF</td>
<td>0.107</td>
<td>1.871</td>
<td>0.062</td>
<td>FF</td>
<td>0.027</td>
<td>0.613</td>
<td>0.540</td>
</tr>
<tr>
<td>H1a(ii) Expertise2 (\rightarrow) (-) Reactance</td>
<td>CIO gender</td>
<td>M</td>
<td>−0.011</td>
<td>0.360</td>
<td>0.719</td>
<td>F</td>
<td>−0.022</td>
<td>1.197</td>
<td>0.232</td>
</tr>
<tr>
<td></td>
<td>CIO (\Sum) Employee gender</td>
<td>MF</td>
<td>−0.018</td>
<td>0.432</td>
<td>0.666</td>
<td>FM</td>
<td>−0.051</td>
<td>2.016</td>
<td>0.044</td>
</tr>
<tr>
<td></td>
<td>CIO (\Sum) Employee gender</td>
<td>MF</td>
<td>0.007</td>
<td>0.137</td>
<td>0.891</td>
<td>FF</td>
<td>0.039</td>
<td>1.129</td>
<td>0.259</td>
</tr>
<tr>
<td>H2a(i) Transformational (\rightarrow) Intention</td>
<td>CIO gender</td>
<td>M</td>
<td>0.274</td>
<td>5.034</td>
<td>0.000</td>
<td>F</td>
<td>0.380</td>
<td>5.309</td>
<td>0.000</td>
</tr>
<tr>
<td></td>
<td>CIO (\Sum) Employee gender</td>
<td>MM</td>
<td>0.200</td>
<td>3.188</td>
<td>0.002</td>
<td>FM</td>
<td>0.439</td>
<td>4.710</td>
<td>0.000</td>
</tr>
<tr>
<td></td>
<td>CIO (\Sum) Employee gender</td>
<td>MF</td>
<td>0.409</td>
<td>4.378</td>
<td>0.000</td>
<td>FF</td>
<td>0.293</td>
<td>3.203</td>
<td>0.001</td>
</tr>
<tr>
<td>H2a(ii) Transformational (\rightarrow) Reactance</td>
<td>CIO gender</td>
<td>M</td>
<td>0.185</td>
<td>3.019</td>
<td>0.003</td>
<td>F</td>
<td>0.072</td>
<td>1.154</td>
<td>0.249</td>
</tr>
<tr>
<td></td>
<td>CIO (\Sum) Employee gender</td>
<td>MM</td>
<td>0.208</td>
<td>2.791</td>
<td>0.005</td>
<td>FM</td>
<td>0.015</td>
<td>0.270</td>
<td>0.787</td>
</tr>
<tr>
<td></td>
<td>CIO (\Sum) Employee gender</td>
<td>MF</td>
<td>0.113</td>
<td>0.974</td>
<td>0.330</td>
<td>FF</td>
<td>0.107</td>
<td>0.990</td>
<td>0.322</td>
</tr>
<tr>
<td>H3a(i) Transactional (\rightarrow) Intention</td>
<td>CIO gender</td>
<td>M</td>
<td>0.310</td>
<td>5.418</td>
<td>0.000</td>
<td>F</td>
<td>0.344</td>
<td>3.934</td>
<td>0.000</td>
</tr>
<tr>
<td></td>
<td>CIO (\Sum) Employee gender</td>
<td>MM</td>
<td>0.276</td>
<td>5.312</td>
<td>0.000</td>
<td>FM</td>
<td>0.276</td>
<td>1.810</td>
<td>0.071</td>
</tr>
<tr>
<td></td>
<td>CIO (\Sum) Employee gender</td>
<td>MF</td>
<td>0.382</td>
<td>3.515</td>
<td>0.000</td>
<td>FF</td>
<td>0.423</td>
<td>4.479</td>
<td>0.000</td>
</tr>
<tr>
<td>H3a(ii) Transactional (\rightarrow) Reactance</td>
<td>CIO gender</td>
<td>M</td>
<td>0.214</td>
<td>3.216</td>
<td>0.001</td>
<td>F</td>
<td>0.342</td>
<td>4.484</td>
<td>0.000</td>
</tr>
<tr>
<td></td>
<td>CIO (\Sum) Employee gender</td>
<td>MM</td>
<td>0.193</td>
<td>2.909</td>
<td>0.004</td>
<td>FM</td>
<td>0.363</td>
<td>4.018</td>
<td>0.000</td>
</tr>
<tr>
<td></td>
<td>CIO (\Sum) Employee gender</td>
<td>MF</td>
<td>0.187</td>
<td>1.397</td>
<td>0.163</td>
<td>FF</td>
<td>0.299</td>
<td>2.401</td>
<td>0.017</td>
</tr>
</tbody>
</table>

Source(s): Authors' creation/work
more pronounced for male CIOs than female CIOs. This effect was corroborated by both structural analysis and MGA analysis, thus confirming H1a(i).

Additionally, this effect exhibited significantly greater strength within the subgroup of male CIOs with female employees when contrasted with the subgroup of male CIOs with male employees. Conversely, it was significantly weaker within the subgroup of female CIOs with male employees compared to the female CIOs with female employees, thus providing support for H1a(ii).

Regarding H1b(i), the findings suggest that there is no notable distinction in the impact of the quadratic effect of CIO IT expertise on reactance between male and female CIOs. Nevertheless, delving into the same effect within subgroups makes it apparent that male employees than female employees discount female CIOs’ expertise more – which is consistent with our hypothesis – FM < FF. Contrary to the expected relationship in the first part of H1b(ii), we discovered that MM > MF, showing that male employees have a much more pronounced lowering of reactance for male CIOs than female employees.

The results of the MGA provide full support for H2b(ii) and partial support for H2a(ii) in the context of gender and transformational leadership style. H2b(i) receives weak support, as it is backed only by structural moderation analysis, not MGA analysis. However, H2a(i) is not supported.

H2a(i) and H2b(ii) demonstrate that the transformational leadership style does not lead to higher intentions among female CIOs. However, as hypothesized, it does elicit more reactance in male CIOs than their female counterparts. This outcome is substantiated by the evidence of structural moderation in H2b(i). H2a(ii) reveals that female employees exhibit lower intentions toward transformational male CIOs when compared to the subgroup of male CIOs with male employees. Additionally, the findings from H2b(ii) indicate that the transformational leadership style of a CIO generates significantly more reactance in the subgroup of male CIOs with female employees than in the subgroup of male CIOs with male employees. It also results in significantly less reactance in the subgroup of female CIOs with male employees compared to the subgroup of female CIOs with female employees. One contrasting discovery in the second part of H2a(ii) is that male employees express lower intentions toward transformational female CIOs compared to the subgroup of female CIOs with female employees.

Even though H3a(i) is reverse supported in MGA analysis, showing that contrary to the hypothesized argument that transactional female CIOs face lower intentions, we found that it is rather transactional male CIOs as opposed to transactional female CIOs who experience lower intentions. The stereotypical factors are more apparent in the subgroup analysis, though – the support for H3a(ii) shows that a transactional style of a CIO leads to higher intentions for female employees – male CIOs as compared to male CIO-male employees’ subgroup and significantly lower intentions for male employees for a transactional female CIO as compared to the female CIO-female employees’ subgroup.

Similarly, H3b(i) is not supported, showing that there is no significant difference in the transactional leadership style of a CIO on reactance based on the gender of the CIO alone. However, the subgroup analysis in H3b(ii) reveals that contrary to the hypothesized argument, it is the transactional male CIO-female employees who experience higher reactance as compared to male CIO-male employees’ subgroup; and also, male employees have lower reactance for transactional female CIO as compared to female CIO-female employees’ subgroup.

Overall, the results confirm the presence of gender stereotypes and the role of stereotype internalization experienced by men and women differently, as hypothesized.

We also control for various factors impacting the employees’ reactance and compliance intentions in the model. Table 5 reports the results for control variables. Significant findings associated with attitude towards the women scale (AWS) and social desirability bias (SDB)
suggest that it is beneficial to control for these factors. AWS (SDB) didn’t impact intention (reactance) but increased reactance (intention) for all groups and subgroups. Threat susceptibility didn’t impact intention but increased reactance for all (except for the MF subgroup). Prior victimization status did not impact intention or reactance in any of the four groups – except for positively impacting reactance for female CIOs. Employee age impacts compliance intentions only for MM and MF subgroups. In contrast, employee age does not impact reactance except for the MM subgroup. Consistent with prior literature (e.g. Feng et al., 2019b), reactance is negatively associated with compliance intentions. However, the structural analysis shows that the effect is weaker for the female CIO and FF groups.

<table>
<thead>
<tr>
<th>Path</th>
<th>CIO/Employee gender</th>
<th>Path coeff</th>
<th>T-stat</th>
<th>Sig</th>
<th>Group</th>
<th>Path coeff</th>
<th>T-stat</th>
<th>Sig</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXP → INT</td>
<td>CIO gender (♂)</td>
<td>M</td>
<td>0.384</td>
<td>5.140</td>
<td>0.000</td>
<td>F</td>
<td>0.339</td>
<td>4.454</td>
</tr>
<tr>
<td></td>
<td>CIO-Employee</td>
<td>MM</td>
<td>0.401</td>
<td>4.692</td>
<td>0.000</td>
<td>FM</td>
<td>0.335</td>
<td>3.455</td>
</tr>
<tr>
<td></td>
<td>Gender</td>
<td>MF</td>
<td>0.284</td>
<td>2.280</td>
<td>0.023</td>
<td>FF</td>
<td>0.313</td>
<td>2.718</td>
</tr>
<tr>
<td>EXP → (−)</td>
<td>CIO gender (♂)</td>
<td>M</td>
<td>−0.038</td>
<td>0.414</td>
<td>0.679</td>
<td>F</td>
<td>−0.046</td>
<td>0.717</td>
</tr>
<tr>
<td>RCT</td>
<td>CIO-Employee</td>
<td>MM</td>
<td>0.002</td>
<td>0.021</td>
<td>0.983</td>
<td>FM</td>
<td>−0.011</td>
<td>0.128</td>
</tr>
<tr>
<td></td>
<td>Gender</td>
<td>MF</td>
<td>−0.042</td>
<td>0.298</td>
<td>0.766</td>
<td>FF</td>
<td>0.000</td>
<td>0.000</td>
</tr>
<tr>
<td>AWS → INT</td>
<td>CIO Gender (♂)</td>
<td>M</td>
<td>−0.002</td>
<td>0.038</td>
<td>0.970</td>
<td>F</td>
<td>−0.059</td>
<td>0.766</td>
</tr>
<tr>
<td>INT</td>
<td>CIO-Employee</td>
<td>MM</td>
<td>−0.022</td>
<td>0.320</td>
<td>0.749</td>
<td>FM</td>
<td>−0.120</td>
<td>1.152</td>
</tr>
<tr>
<td></td>
<td>Gender</td>
<td>MF</td>
<td>0.125</td>
<td>1.095</td>
<td>0.274</td>
<td>FF</td>
<td>0.047</td>
<td>0.438</td>
</tr>
<tr>
<td>AWS → RCT</td>
<td>CIO Gender (♂)</td>
<td>M</td>
<td>0.368</td>
<td>3.988</td>
<td>0.000</td>
<td>F</td>
<td>0.304</td>
<td>4.172</td>
</tr>
<tr>
<td>RCT</td>
<td>CIO-Employee</td>
<td>MM</td>
<td>0.252</td>
<td>2.257</td>
<td>0.024</td>
<td>FM</td>
<td>0.291</td>
<td>4.007</td>
</tr>
<tr>
<td>SCP → INT</td>
<td>CIO Gender (♂)</td>
<td>M</td>
<td>−0.029</td>
<td>0.470</td>
<td>0.638</td>
<td>F</td>
<td>0.107</td>
<td>1.787</td>
</tr>
<tr>
<td>SCP → RCT</td>
<td>CIO Gender (♂)</td>
<td>M</td>
<td>0.188</td>
<td>2.057</td>
<td>0.040</td>
<td>F</td>
<td>0.308</td>
<td>4.648</td>
</tr>
<tr>
<td>VIC → INT</td>
<td>CIO Gender (♂)</td>
<td>M</td>
<td>0.023</td>
<td>0.878</td>
<td>0.381</td>
<td>F</td>
<td>0.060</td>
<td>1.863</td>
</tr>
<tr>
<td>VIC → RCT</td>
<td>CIO Gender (♂)</td>
<td>M</td>
<td>0.040</td>
<td>1.285</td>
<td>0.199</td>
<td>F</td>
<td>0.067</td>
<td>1.965</td>
</tr>
<tr>
<td>SDB → INT</td>
<td>CIO Gender (♂)</td>
<td>M</td>
<td>0.198</td>
<td>2.974</td>
<td>0.003</td>
<td>F</td>
<td>0.236</td>
<td>4.618</td>
</tr>
<tr>
<td>SDB → RCT</td>
<td>CIO Gender (♂)</td>
<td>M</td>
<td>0.247</td>
<td>4.798</td>
<td>0.013</td>
<td>F</td>
<td>0.340</td>
<td>2.936</td>
</tr>
<tr>
<td>AGE → INT</td>
<td>CIO gender (♂)</td>
<td>M</td>
<td>0.000</td>
<td>0.005</td>
<td>0.996</td>
<td>F</td>
<td>0.037</td>
<td>1.341</td>
</tr>
<tr>
<td>AGE → RCT</td>
<td>CIO Gender (♂)</td>
<td>M</td>
<td>−0.119</td>
<td>2.362</td>
<td>0.019</td>
<td>FM</td>
<td>0.231</td>
<td>3.126</td>
</tr>
<tr>
<td>RCT → (−)</td>
<td>CIO gender (♂)</td>
<td>M</td>
<td>−0.009</td>
<td>0.111</td>
<td>0.912</td>
<td>F</td>
<td>−0.023</td>
<td>0.729</td>
</tr>
<tr>
<td>INT</td>
<td>CIO-Employee</td>
<td>MM</td>
<td>0.041</td>
<td>0.405</td>
<td>0.688</td>
<td>FM</td>
<td>−0.139</td>
<td>1.160</td>
</tr>
<tr>
<td></td>
<td>Gender</td>
<td>MF</td>
<td>−0.278</td>
<td>1.494</td>
<td>0.136</td>
<td>FF</td>
<td>−0.352</td>
<td>2.244</td>
</tr>
</tbody>
</table>

Table 5. Control variables results

Note(s): Construct abbreviations are explained in Appendix 2
Source(s): Author’s creation/work
6. Discussion and conclusion

Our work extends the understanding of gender issues in information security compliance and IT in general by examining how male and female IT leaders are characterized by men and women based on their gender role internalization. Thus, our research creates awareness of the extent of stereotyping and society’s expectations of gender roles and one’s internalization of these expectations while at the same time responding to the calls to examine social inclusion issues in the IT field (Jia et al., 2022) and thus understand the cognitive processes contributing to the lack of female representation in leadership positions (Giacomin et al., 2022).

Our findings provide several important theoretical, social and practical implications based on gender stereotypes and social role theory (Eagly and Wood, 2012). We explain our contributions in the context of the internalization of gender role stereotypes, glass ceiling effects, double bind and Simpson’s paradox below.

6.1 Theoretical implications

First, our work shows that organizational leadership and, particularly, gender could influence employees’ compliance with security policy and that such relationships are also a function of employee gender. It thus adds to the IT security compliance literature and our understanding of the sender’s characteristics in enhancing IT security compliance (Bansal et al., 2023; Feng et al., 2019a).

Second, our research findings suggest that men and women have different biases and expectations regarding expertise due to the socialization of gender roles. Our results reveal that male employees adhere “vigorously” (Hentschel et al., 2019, p. 4) to the stereotypes that benefit them and lower reactance to the expertise (in quadratic form) of male CIOs while undervaluing female CIOs’ expertise and showing less compliance intention. In contrast, female employees are more willing to comply with male CIOs’ expertise but less so with female CIOs’ expertise due to self-doubt and internalized stereotypes. In addition, Our work shows that the stereotypes are more evident at the quadratic level of expertise, as predicted by the glass ceiling theory (Cotter et al., 2001). Thus, our work adds to the reports (e.g. Igbaria and Baroudi, 1995) and confirms the existence of glass ceiling impediments in IT.

Third, our study contributes to the leadership literature by showing how gender roles influence employees’ reactions to different leadership styles in the context of IT security compliance. The findings reveal that female employees have higher (lower) compliance intentions for transactional (transformational) male CIOs while more (less) reactance to transformational male (female) CIOs. Further, the finding that transactional female CIOs and transformational female CIOs both have lower intentions with male employees highlights the “double bind” (Eagly and Carli, 2012, p. 149), where female leaders are punished for being too communal or being too agentic.

Fourth, our findings help explain that the obstacles to the career progression of female leaders and CIOs, termed the Glass Ceiling, could be related to undervaluing their influence by their colleagues and subordinates, a phenomenon we describe as sticky floors. We use this term to describe how female leaders, especially CIOs, face persistent challenges in their recognition and effectiveness from their subordinates due to gender biases, which limit their career progression. The “glass ceiling” was first coined by Marilyn Loden in 1978 to denote the gender or racial disparities in opportunities for advancing to higher-level positions (Cotter et al., 2001). The “sticky floors” concept explains how subordinates hinder and undermine female leaders, especially CIOs, making their career journey more difficult and less rewarding. We redefine “sticky floors” as the challenges women leaders face in reaching higher positions, where their expertise and influence are discounted and undervalued by peers and subordinates. This concept highlights factors contributing to gender disparities in corporate leadership, often associated with the glass ceiling effect.
Lastly, our study demonstrates that employee gender is crucial for understanding the effects of leaders’ gender such that the employee gender influences the stereotype influence of the CIO gender. We thus report a Simpson’s paradox related to employee gender, which adds to the literature where such effects are found, for example, Albers (2015) and Solórzano et al. (2002). Simpson’s paradox is defined as “a statistical phenomenon where an association between two variables in a population emerges, disappears or reverses when the population is divided into subpopulations” (Sprenger and Weinberger, 2021, p. 1).

6.2 Social implications
The results of our study reveal the underlying sources of the stereotypes and their effects on our society. Our work provides several social implications:

First, we find some positive signs that older individuals, who may hold more traditional gender role stereotypes, favor male CIOs more than younger individuals (i.e. a positive association between age and intentions within MM and MF groups), suggesting that younger generations are witnessing a change in these stereotypes.

Second, our findings reveal that female CIOs exhibiting either transactional or transformational leadership may encounter lower compliance intentions from male employees, which underscores the workplace double bind women often face. The term “double bind” refers to a paradox involving conflicting expectations: when women express warmth, they risk being perceived as too soft, while expressing assertiveness may lead to perceptions of harshness or aggression—a situation aptly captured by the phrase “damned if you do, doomed if you don’t” (Catalyst, 2007, p. 1).

Third, the social implications of subordinates undervaluing a female leader’s expertise and influence, a concept we refer to as a sticky floor, are significant. This phenomenon shows how gender bias and stereotypes limit career progression for female leaders and contribute to a less equitable society. The lack of recognition of female leaders creates a vicious cycle, which can affect the aspirations of future generations of female leaders, limiting their career ambitions.

Our findings underscore the need for broader societal change at both organizational and societal levels to combat gender bias and promote equality.

6.3 Practical implications
Our findings have several direct practical implications related to leadership style and the underappreciated expertise of female IT leaders. Firstly, our research demonstrates that female leaders receive insufficient recognition from their team members. To overcome this, organizations must empower their female leaders by acknowledging their expertise openly and celebrating their accomplishments publicly. By facilitating the enhanced visibility, recognition and influence of female IT leaders, organizations can effectively surmount obstacles and foster a workplace culture that is more inclusive and diverse. Female leaders getting diminished recognition for their expertise also provides another perspective to help explain a question raised in Forbes magazine by Chamorro-Premuzic (2021), “If Women Are Better Leaders, Then Why Are They Not In Charge?”

Secondly, our research underscores the significance of championing various leadership approaches to create awareness that transformational leadership, which revolves around inspiration and motivation, is not exclusive to women. This approach aims to diminish the tendency for women to perceive that they should exclusively adopt transformational leadership and likewise for men. This awareness of the value of both styles, with a particular emphasis on transformational leadership, becomes increasingly critical in the era of AI, as empathy is recognized as the most highly coveted human skill (Meister, 2019).
Thirdly, our study suggests that female CIOs can overcome the double bind they often face by displaying assertiveness. Our results reveal that, on the whole, it appears that female CIOs with a transactional leadership style tend to garner greater support than their male counterparts with similar leadership approaches.

To summarize, our research emphasizes the importance of organizations and individuals taking proactive steps to advance gender equality and create atmospheres that encourage women to be acknowledged for their accomplishments—a challenge with vast economic implications exceeding 12 trillion dollars (McKinsey and Co, 2015). It also underscores the need to educate both men and women about the broader social consequences of internalizing gender roles that go beyond the organizational setting. Organizations can implement various measures, including mentorship programs, support networks and efforts to confront and disassemble detrimental stereotypes and biases. It is crucial for both men and women to reflect on and understand how they can modify their behavior to foster social inclusion.

6.4 Limitations and future research

Our investigation has several limitations that offer opportunities for future studies. The research question was focused on how leadership characteristics influence employees’ intended information security behavior, considering the combination of CIO and employee gender. Although the chosen design of our study enables the isolation of particular constructs of interest, our research design is unable to truly capture social, cultural and organizational aspects related to information security behavior within a complex organizational environment. For example, we are unable to capture the variation in the company’s culture and value, type of industry, business model, organizational structure, size and CIO profile. We acknowledge that such variables, along with the organizational culture and the espoused national cultural orientations of the employees, may also directly impact how employees internalize the congruence of female CIO’s security recommendations. However, our study only focuses on U.S. companies because we specified the U.S. location requirements for our M-Turk respondents. Future research could employ designs that address psychological factors and organizational characteristics, exploring these effects in diverse cultures and field settings. Additionally, our nomological model could be expanded by examining alternative mediators or moderators, including stereotypes related to race, age and their combinations with gender. Future research can explore the prevalence of sticky floors in other contextual settings and domains.

6.5 Conclusion

In conclusion, our research broadens the understanding of gender issues in IT security compliance and IT in general. We examined how male and female IT leaders are perceived based on their gender role internalization, highlighting the pervasive nature of stereotyping and societal expectations of gender roles. Our findings have significant theoretical, social and practical implications, contributing to the literature on IT security compliance, leadership and gender studies. More importantly, our research underscores the need for continued efforts to address gender biases and promote social inclusion in the IT field.

References


Chamorro-Premuzic, T. (2021), “If women are better leaders, then Why are they not in Charge?”, available at: https://www.forbes.com/sites/tomaspremuzic/2021/03/07/if-women-are-better-leaders-then-why-are-they-not-in-charge/?sh=518789dab6c88 (accessed 23 October 2023).


Challenges for female CIOs


Challenges for female CIOs


(The Appendix follows overleaf)
Please read the following conversation between Kyle, who works for ABC
Corporation and Ben, his friend from college
Kyle: Hi Ben, I got news from my company to share with you!
Ben: Go ahead!
Kyle: Recently, our company hired a new CIO – Mary Jane (Michael Smith). The new
CIO comes with 15 years of strong experience as a director of IT, including cyber
security in a reputed Fortune 500 company, and has a master’s degree in Information
Technology from an ivy league institution
Ben: Great! It seems your new CIO has quite some experience in the IT area
Kyle: Yes, the new CIO gave a recent presentation to all of us and shared that being
cyber-alert and cyber-safe is very important to our company as it helps keep our
customer information and intellectual property safe
Ben: I think the CIO wants to protect the company’s IT infrastructure and information
CIO low expertise
Please read the following conversation between Kyle, who works for ABC
Corporation, and Ben, his friend from college
Kyle: Hi Ben, I got news from my company to share with you!
Ben: Go ahead!
Kyle: Recently, our company hired a new CIO – Mary Jane (Michael Smith). The new
CIO has 7 years of experience in project management but little experience in IT and
cyber security. The new CIO implemented IT security policies and guidelines for
employees to protect customer information and intellectual property
Ben: I think a CIO’s job is to protect a company’s IT infrastructure and information

Please read the continued conversation between Kyle and Ben about Kyle’s new CIO
Kyle: The new CIO instills confidence in us about our IT security performance. The
CIO suggests that cyberattacks are on the rise. The effect of such an attack could be
devastating to our company. We cannot afford to lose customer data or risk a
ransomware attack. The CIO, in a meeting, mentioned that phishing scams are a
major reason for ransomware and other major data breaches. To keep our
information secured, CIO always motivates employees and recommends always
being careful when clicking on links in any email
Ben: The CIOs worldwide are worried about their organization’s cybersecurity; that’s
so true
Kyle: However, another day, one of my colleagues accidentally clicked on a phishing
email. It was fortunate that the phishing email didn’t do much damage to our network
security. Our new CIO reached out to my colleague to discuss if anything can be done
to prevent such incidents from happening to my colleague and others in the
organization. After the conversation, the new CIO arranged for my colleague to
undergo a short training on staying cyber-safe and avoiding getting scammed by
phishing emails and messages
Ben: Well, I am glad your new CIO offered your colleague a chance to learn from this
lesson. Your new CIO went the extra mile to earn the respect of the employees while
also ensuring that IT security is not compromised

Table A1.
Vignettes (continued)
Kyle: The CIO further said that cyberattacks are on the rise. The effect of such an attack could be devastating to our company. We cannot afford to lose customer data or risk a ransomware attack. The CIO mentioned that phishing scams are a major reason for ransomware and other major data breaches. Our new CIO always seems to emphasize the importance of complying with security policies. To keep our information secured, CIO requires we always be careful when clicking on links in any email.

Ben: The CIOs worldwide are worried about their organization's cybersecurity; that's so true.

Kyle: However, another day, one of my colleagues accidentally clicked on a phishing email. It was fortunate that the phishing email didn't do much damage to our network security. However, our new CIO got my colleague fined two weeks of a pay cut and a carelessness note attached to the personnel file.

Ben: I am very sorry to hear that. It is unfortunate that it happened to your colleague who has to face this penalty. Your new CIO is a leader who uses penalties and rewards rather than inspiring employees to strive beyond required expectations. Leaders like your new CIO are more focused on task attainment and less concerned about earning the respect of their employees.

Kyle: Seems you are right.
### Construct Items

<table>
<thead>
<tr>
<th>Construct</th>
<th>Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expertise (EXP)</td>
<td>EXP1 The CIO seems to be knowledgeable about cybersecurity</td>
</tr>
<tr>
<td></td>
<td>EXP2 The CIO seems to be an expert in IT</td>
</tr>
<tr>
<td></td>
<td>EXP3 The CIO seems to be knowledgeable about IT</td>
</tr>
<tr>
<td>Intention (INT)</td>
<td>INT1 If I were in Kyle’s place, I would follow the new CIO's cybersecurity recommendations</td>
</tr>
<tr>
<td></td>
<td>INT2 If I were Kyle, I would comply with the new CIO’s cybersecurity recommendations</td>
</tr>
<tr>
<td></td>
<td>INT3 I predict that, if I were Kyle, I would follow the new CIO’s cybersecurity recommendations</td>
</tr>
<tr>
<td></td>
<td>INT4 If I were Ben, I would advise Kyle to follow the new CIO’s cybersecurity recommendations</td>
</tr>
<tr>
<td></td>
<td>INT5 I predict that, if I were Ben, I would advise Kyle to follow the new CIO’s cybersecurity recommendations</td>
</tr>
<tr>
<td>Reactance (RCT)</td>
<td>RCT1 If I were Kyle, the IT security recommendation made by the new CIO would trigger a sense of resistance in me</td>
</tr>
<tr>
<td></td>
<td>RCT2 If I were Kyle, I would want to contradict the new CIO’s IT security</td>
</tr>
<tr>
<td></td>
<td>RCT3 If I were Kyle, the IT security recommendation made by the new CIO would make me want to do the opposite of what it instructed me to do</td>
</tr>
<tr>
<td></td>
<td>RCT4 I would consider the security recommendations made by Kyle’s new CIO as an intrusion</td>
</tr>
<tr>
<td></td>
<td>RCT5 I would resist the IT security recommendation suggested by Kyle’s new CIO</td>
</tr>
<tr>
<td>Leadership style:</td>
<td>TRF1 I believe that Kyle’s new CIO spent time mentoring and coaching the employees for future performance</td>
</tr>
<tr>
<td>transformational (TRF)</td>
<td>TRF2 . . . increases an employee’s motivation</td>
</tr>
<tr>
<td>Leadership style:</td>
<td>TRC1 . . . focuses on certain conditions required to achieve a reward (or pay increase) or avoid penalty (or pay cut)</td>
</tr>
<tr>
<td>transactional (TRC)</td>
<td>TRC2 . . . expresses the implications of the employee meeting (or not meeting)</td>
</tr>
<tr>
<td>Attitude towards women</td>
<td>AWS1 There are many jobs in which men should be given preference over scale (AWS)</td>
</tr>
<tr>
<td>scale (AWS)</td>
<td>AWS2 The intellectual leadership of a community should be largely in the hands of men</td>
</tr>
<tr>
<td>Phishing susceptibility (SCP)</td>
<td>SCP1 I am at risk of falling victim to a phishing attack</td>
</tr>
<tr>
<td></td>
<td>SCP2 It is likely that I will fall victim to a phishing attack</td>
</tr>
<tr>
<td>Social desirability bias (SDB)</td>
<td>SDB1 I never cover up my mistakes</td>
</tr>
<tr>
<td></td>
<td>SDB2 I don’t gossip about other people’s business</td>
</tr>
<tr>
<td>Victim of a phishing attack (VIC)</td>
<td>VIC1 I personally fell victim to a phishing attack before (yes/maybe/no)</td>
</tr>
<tr>
<td>Marker variable (MKR)</td>
<td>MKR1 I always try to imagine how my life might have been different</td>
</tr>
</tbody>
</table>

**Table A2.** Instrument

**Source(s):** Refer to Appendix 3
Appendix 3

Experiment flow

1. Read and agree to the IRB consent form
2. Read the two CIO vignettes – one out of four related to expertise (M/F; High/Low) and one out of four related to leadership style (M/F; Transformational/Transactional)
3. Attention check and manipulation questions
4. Measured expertise, leadership style, intention, reactance
5. Attention check questions
6. Measured demographic variables
7. Survey end

Source(s): Authors’ creation/work

Appendix 4

Common method variance
Using the marker variable (MKR1), we found the second-lowest positive correlation between the marker variable and the latent constructs to be 0.000. Also, the outer VIFs in the SEM-PLS analysis for the male and female CIO groups were less than 2.323 and 3.218, respectively (MM max value: 2.735; MF max value: 2.280; FM max value: 3.571; FF max value: 3.185) and all were less than the suggested cutoff value of 5.0 (Sarstedt et al., 2021). That provides additional confidence that the CMV threat did not seriously impact our data.

Source(s): Authors’ creation/work

Corresponding author
Gaurav Bansal can be contacted at: bansalg@uwgb.edu

For instructions on how to order reprints of this article, please visit our website: www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: permissions@emeraldinsight.com