مجلة الاسكندرية للبحوث المحاسبية
قسم المحاسبة والمراجعة

العدد الثالث – سبتمبر 2022 – المجلد السادس

قياس أثر الثالوث المظلم كسمات شخصية على اتجاهات المحاسبين نحو الإفصاح عن مخاطر الأمن السيبراني: دراسة شبه تجريبية

د/ عارف محمود كامل عيسى
أستاذ مساعد بقسم المحاسبة
كلية التجارة – جامعة القاهرة

د/ سمير إبراهيم عبد العظيم محمد
مدرس بقسم المحاسبة
كلية التجارة – جامعة بني سويف

ملخص البحث

يتمثل الهدف الرئيس لهذه الدراسة في قياس أثر الثالوث المظلم (الميكافيللية–النرجسية– السيكوباتية) كسمات شخصية على اتجاهات المحاسبين نحو الإفصاح عن مخاطر الأمن السيبراني. لتحقيق هذا الهدف قام الباحثان بإجراء دراسة شبه تجريبية على عينة من المحاسبين العاملين لدى بعض البنوك الكبرى في جمهورية مصر العربية، وقد بلغ حجم العينة النهائي 101 محاسب، وقد تم تحليل بيانات الدراسة إستناداً لأساليب الإحصاء الوصفي، والإنحدار الخطي بطريقة المربعات الصغرى OLS Regression. وقد توصل الباحثان لوجود تأثير معنوي للثالوث المظلم على اتجاهات المحاسبين نحو الإفصاح عن مخاطر الأمن السيبراني، وقد اتضح هذا التأثير عند فحص الميكافيللية والنرجسية، حيث أكدت النتائج على تزايد درجة قبول المحاسبين للإفصاح عن مخاطر الأمن السيبراني، كلما زاد مستوى الميكافيللية والنرجسية كسمات شخصية لديهم، في نفس الوقت يقترن هذا القبول بنغمة إفصاح إيجابية ومحاولات أكبر للتلاعب عند الإفصاح عن مخاطر الأمن السيبراني، في محاولة منهم لإخفاء الجوانب السلبية والإفصاح بشكل أكبر عن النواحي الإيجابية وإظهارها لمستخدمي المعلومات. لذلك، تم قبول الفرض الأول (H1) والثاني (H2) للدراسة. أما بخصوص السيكوباتية فلم يُلاحظ الباحثان أي تأثير معنوي لها على اتجاهات المحاسبين نحو الإفصاح عن مخاطر الأمن السيبراني، وترجع تلك النتيجة لإنخفاض مستوى السيكوباتية لدى عينة الدراسة وهو ما اتضح عند إجراء إختبار One Sample t–test، فقد إنخفض متوسط مؤشر السيكوباتية عن القيمة المحايدة "3" على مقياس ليكرت الخماسي بشكل معنوي. لذا، تم رفض الفرض الثالث للدراسة (H3). تُعد نتائج هذه الدراسة مفيدة للباحثين والمستثمرين ومراقبى الحسابات والجهات التنظيمية، وغيرهم من أصحاب المصالح الآخرين حول الآثار السلبية المحتملة للثالوث المظلم كسمات شخصية على اتجاهات المحاسبين نحو الإفصاح عن مخاطر الأمن السيبراني.

الكلمات المفتاحية: الثالوث المظلم، الميكافيللية، النرجسية، السيكوباتية، الإفصاح عن مخاطر الأمن السيبراني.

E.mail: aref_mahmoud_issa@foc.cu.edu.eg
E.mail: samir.mohamed@commerce.bsu.edu.eg

The Effect of Dark Triad as Personality Traits on Accountants' Attitude toward CyberSecurity Risks Disclosure: A Quasi-Experimental Study in Egypt

Abstract

The main objective of this study is to measure the effect of the dark triad (Machiavellianism- narcissism- psychopathy) as personality traits on accountants' attitudes towards cyber security risks disclosure. To achieve this objective, we have conducted a quasi-experimental study depending on a sample of accountants in some Egyptian banks. The final sample size was 101 accountants, and the study data were analyzed based on the descriptive statistics, and OLS Regression. The results confirm a significant relation between the dark triad and accountants' attitudes toward cybersecurity risks disclosure, this relation was obvious when examining Machiavellianism and narcissism. The results confirm that Machiavellianism and narcissism are accepting cyber security risks disclosure. This acceptance are accompanied by positive tone in cyber security risks disclosure and greater attempts to manipulate cyber security risks disclosures, they endeavor to hide the negative cyber security information and disclose more about the positive information. Therefore, the first and second hypotheses (H1&H2) were accepted. As for psychopathy, we did not find any significant relation between psychopathy and accountants' attitudes toward cyber security risks disclosure, this results can be explained due to the lower level of psychopathy in our sample, which was clear after conducting one sample t-test. The psychopathy index mean was significantly lower than the neutral value "3" on the Likert scale, so the third hypothesis (H3) was rejected. Our results are useful to researchers, investors, auditors, regulators, and other stakeholders regarding the potential negative effects of the dark triad as personality traits on accountants' attitudes toward cybersecurity risks disclosure.

Keywords: Dark triad, Machiavellianism, Narcissism, Psychopathy, Cybersecurity risks disclosure.

1- الإطار العام للدراسة

1-1 مقدمة

بين الحين والآخر، تظهر بعض الفضائح والانهيارات المالية التي تتسبب في خسائر فادحة للمستثمرين ويكون لها صدى سلبي واسع على أسواق رأس المال، ومن أشهرها انهيار Enron الأمريكية عام 2002، والأزمة المالية العالمية عام 2008، وأخيراً إفلاس Wirecard الألمانية عام 2020 (Davies 2020). في الكثير من الأحيان ترتبط تلك الفضائح بتورط الإدارة العليا في العديد من الممارسات الاحتيالية لخدمة مصالحها الخاصة، وحجب تلك الممارسات لفترات طويلة من الزمن (Mutschmann et al. 2021).

تؤكد النظرية النفسية Psychological Theory على أنه لكي يتمكن أي فرد من مواكبة عملية احتيال طويلة المدى بنجاح، فإن ذلك يتطلب ميول نفسية تدفعه لصنع هذا القرار غير الأخلاقي من أجل تحقيق مكاسب شخصية مثل؛ الكذب، والقسوة وإنعدام الضمير، وعدم الشعور بالذنب، والشعور بالتفرد. تلك السمات تنتشر بشكل كبير بين مرتكبي جرائم الإحتيال (Clarke 2005; Kirkman 2005; Babiak and Hare 2006; Corry et al. 2008; Ramamoorti 2008; Stevens et al. 2012; Boddy 2015). وتُعد الميكافيللية والنرجسية والسيكوباتية من أبرز السمات الشخصية المظلمة والتي ترتبط بدرجة كبيرة بالسلوكيات غير الأخلاقية في منشآت الأعمال (Paulhus and Jones 2002; Mutschmann et al. 2021).

لذا اتجه بعض الباحثين في الآونة الأخيرة لفحص الإنعكاسات المحاسبية للثالوث المظلم- أو أحد عناصره- كسمات شخصية للمديرين التنفيذيين والماليين في منشآت الأعمال، حيث تناول الباحثون أثر الثالوث المظلم على ممارسات إدارة الأرباح (Olsen et al. 2014; Ham et al. 2017)، والغش المحاسبي (Ramamoorti 2008; Rijsenbilt and Commandeur 2013; Mutschmann et al. 2021)، والممارسات الضريبية التعسفية (Olsen and Stekelberg 2016). وفي مجال الإفصاح الإختياري ركز الباحثون على الإفصاح الإختياري عن توقعات الأرباح (Ma 2015)، ونغمة الإفصاح (Marquez-Illescas et al. 2019)، ومستوى الإفصاح الإختياري (Mashayekh et al. 2021)، وأخيراً الإفصاح عن المبادرات الإجتماعية (Lassoued and Khanchel 2022).

لم تتطرق الدراسات السابقة لفحص أثر الثالوث المظلم –كسمات شخصية للإدارة– على الإفصاح عن مخاطر الأمن السيبراني، كأحد مجالات الإفصاح الإختياري الذي فرض نفسه في الآونة الأخيرة. وبصفة خاصة مع تزايد إعتمادية الدول والمنشآت حول العالم على تكنولوجيا المعلومات والإتصالات في أداء مختلف الأنشطة الإقتصادية، حيث تقوم غالبية المنشآت بتخزين ونقل معلومات مهمة وذات حساسية عالية عبر الشبكات بالإعتماد على الحوسبة السحابية Cloud Computing (Ashraf 2020)، الأمر الذي يفرض تحديات غير عادية على الدول والمنشآت في ظل التهديدات المحتملة لإختراق أنظمتها الإلكترونية (PwC 2017). فعلى سبيل المثال؛ تعرضت أرامكو السعودية لبعض الهجمات الإلكترونية في عام 2012، نتج عنها خسائر فادحة للمنشأة، ولم تستطع إستخدام الإنترنت لمدة خمسة أشهر تقريباً، كما تعرضت بعض البنوك في الإمارات العربية المتحدة، وسلطنة عمان لخسائر فادحة تجاوزت 45 مليون دولار نتيجة سرقة بعض أجهزة الصراف الآلي الإلكترونية (السمحان 2020). كذلك فإن الإختراق الذي حدث لوكالة Equifax الأمريكية في عام 2017 عرَّض بيانات أكثر من 143 مليون فرد أمريكي للتهديد (Yang et al. 2020).

لذا أصبحت مخاطر الأمن السيبراني مصدر قلق كبير لدى مجلس الإدارة، والإدارة التنفيذية، والمراجعين الداخليين، ومراقبي الحسابات، والمستثمرين، وعملاء المنشأة، والجهات التنظيمية (Center for Audit Quality 2016; AICPA 2017c)، وبصفة خاصة مع تطور وتنوع مخاطر الأمن السيبراني (Ashraf 2020). إستجابة لهذه التحديات المتزايدة، أصبح مطلوباً من المنشآت الإفصاح عن مخاطر الأمن السيبراني والجهود التي تبذلها الإدارة في الحد من تلك المخاطر (Newman 2018). ولتحقيق الاتساق في الإفصاح طوَّر المعهد الأمريكي للمحاسبين القانونيين (AICPA) إطاراً لإعداد تقارير الأمن السيبراني، يمكن للمنشآت الإعتماد عليه لتوفير معلومات مفيدة لأصحاب المصالح Stakeholders حول البرامج التي تعتمد عليها المنشأة لإدارة مخاطر الأمن السيبراني وفعاليتها (AICPA 2017a). كما أشارت هيئة تداول الأوراق المالية الأمريكية (SEC) إلى أن مخاطر الأمن السيبراني أصبحت تُشكل تهديداً للمنشآت والعملاء، وأصبحت المعلومات المرتبطة بهذه المخاطر أحد العوامل المؤثرة على أسواق رأس المال (SEC) 2018، لذا فإنه من الأهمية بمكان فهم اتجاهات المحاسبين نحو الإفصاح عن هذه المخاطر والعوامل المؤثرة عليها، وأهمية تنظيمها.

2-1 طبيعة المشكلة

اتجه بعض الباحثين في الآونة الأخيرة لفحص الآثار السلبية للثالوث المظلم كسمات شخصية على جودة التقارير المالية (Ramamoorti 2008; Rijsenbilt and Commandeur 2013; Olsen et al. 2014; Mutschmann et al. 2021; Ham et al. 2017)، بينما اتجه البعض الآخر لفحص الآثار السلبية للثالوث المظلم في مجال الإفصاح الإختياري، حيث لاحظ Mashayekh et al. (2021) إنخفاض مستوى الإفصاح الإختياري لدى المديرين ذوي السمات الشخصية المظلمة، كذلك تنخفض إحتمالية إصدارهم لتوقعات الأرباح (Ma 2015)، وفي حالة الإعلان عن الأرباح فإنهم يعتمدون بشكل أكبر على النغمة الإيجابية (Marquez-Illescas et al. 2019). بل ربُما تكون تلك الإفصاحات إنتقائية بالتركيز على الجوانب الإيجابية وإهمال الجوانب السلبية، كما في حالة الإفصاح عن المبادرات الإجتماعية (Lassoued and Khanchel 2022).

في ضوء ما تقدم، يُلاحظ الباحثان ندرة الدراسات السابقة التي تفحص أثر الثالوث المظلم كسمات شخصية للإدارة على الإفصاح الإختياري بصفة عامة، فضلاً عن الندرة الشديدة في الدراسات- في حدود علمنا- التى اتجهت لفحص أثر الثالوث المظلم على اتجاهات المحاسبين نحو الإفصاح عن مخاطر الأمن السيبراني كأحد الاتجاهات البحثية الجديدة التي حازت على إهتمام الباحثين والجهات التنظيمية في الآونة الأخيرة. ولا يزال هذا النوع من الإفصاح إختيارياً في العديد من الدول حول العالم، بما يجعله أكثر عُرضة للتلاعب من قبل الإدارة، وبصفة خاصة في الأسواق الناشئة مع إنخفاض مخاطر التقاضي، وإنخفاض جودة نظم حوكمة الشركات في تلك الأسواق (Ebaid 2016). لذا فإننا نتوقع أن يؤثر الثالوث المظلم كسمات شخصية للمحاسبين على مدى قبولهم للإفصاح عن مخاطر الأمن السيبراني، ونغمة الإفصاح في حالة تنظيم هذا الإفصاح، وإحتمالية التلاعب في هذه الإفصاحات. وبناءً على ذلك تتمثل التساؤلات البحثية فيما يلي:

- إلى أي مدى يؤثر الثالوث المظلم كسمات شخصية للمحاسبين على مدى قبولهم للإفصاح عن مخاطر الأمن السيبراني؟
- إلى أي مدى يؤثر الثالوث المظلم كسمات شخصية للمحاسبين على نغمة الإفصاح عن مخاطر الأمن السيبراني؟
- إلى أي مدى يؤثر الثالوث المظلم كسمات شخصية للمحاسبين على إحتمالية التلاعب بمعلومات مخاطر الأمن السيبراني؟

1-3 أهمية الدراسة

تستمد هذه الدراسة أهميتها للعديد من الأسباب من أهمها:

أولاً: تُعد هذه الدراسة إمتداداً للدراسات السابقة في مجال الثالوث المظلم والإفصاح الإختياري، كما تُعد –في حدود علمنا– من طليعة الدراسات التي تبحث في أثر الثالوث المظلم كسمات شخصية على اتجاهات المحاسبين نحو الافصاح عن مخاطر الأمن السيبراني في بيئة الأعمال المصرية.

ثانياً: تقدم هذه الدراسة إضافة بحثية مهمة في مجال الثالوث المظلم، والإفصاح عن مخاطر الأمن السيبراني في جمهورية مصر العربية كنموذج للأسواق الناشئة، بالتركيز على اتجاهات المحاسبين نحو الإفصاح عن مخاطر الأمن السيبراني، من حيث مدى قبولهم للإفصاح عن هذه المخاطر، ونغمة الإفصاح التي سيعتمدون عليها، والتلاعب المحتمل في تلك الإفصاحات في حالة تنظيمها.

ثالثاً: تُقدم الدراسة مجموعة من النتائج العملية المفيدة للحد من مخاطر الأمن السيبراني، وتحسين الإفصاح عن هذا النوع من المخاطر، لذا تُعد نتائج هذه الدراسة مفيدة للمنشآت والباحثين ومراقبى الحسابات، والمستثمرين والجهات التنظيمية.

1-4 الهدف من الدراسة

يتمثل الهدف الرئيس للدراسة في قياس أثر الثالوث المظلم كسمات شخصية للمحاسبين على اتجاهاتهم نحو الإفصاح عن مخاطر الأمن السيبراني، وينبثق عن هذا الهدف مجموعة الأهداف الفرعية التالية:

- قياس أثر الثالوث المظلم كسمات شخصية للمحاسبين على مدى قبولهم للإفصاح عن مخاطر الأمن السيبراني.
- قياس أثر الثالوث المظلم كسمات شخصية للمحاسبين على نغمة الإفصاح عن مخاطر الأمن السيبراني.
- قياس أثر الثالوث المظلم كسمات شخصية للمحاسبين على إحتمالية التلاعب بمعلومات مخاطر الأمن السيبراني.

1-5 فروض الدراسة

تتمثل الفروض الرئيسة للدراسة فيما يلي:

- **الفرض الرئيس الأول:** يوجد تأثير إيجابي معنوي للميكافيللية كسمة شخصية للمحاسبين في البنوك العاملة بمصر على اتجاهاتهم نحو الإفصاح عن مخاطر الأمن السيبراني.
- **الفرض الرئيس الثاني:** يوجد تأثير إيجابي معنوي للنرجسية كسمة شخصية للمحاسبين في البنوك العاملة بمصر على اتجاهاتهم نحو الإفصاح عن مخاطر الأمن السيبراني.
- **الفرض الرئيس الثالث:** يوجد تأثير إيجابي معنوي للسيكوباتية كسمة شخصية للمحاسبين في البنوك العاملة بمصر على اتجاهاتهم نحو الإفصاح عن مخاطر الأمن السيبراني.

1-6 حدود الدراسة

لم تتناول الداسة فحص الجوانب الإيجابية للسمات الشخصية المظلمة، بل تم التركيز على الجوانب السلبية الناتجة عن تزايد مستوى تلك السمات بين المحاسبين. كذلك إقتصر الباحثان على فحص اتجاهات المحاسبين نحو الإفصاح عن مخاطر الأمن السيبرانى، بالتركيز على قبول الإفصاح، ونغمة الإفصاح، والتلاعب المحتمل فى الإفصاح عن تلك المخاطر دون التطرق لبعض الجوانب الأخرى فى الإفصاح مثل؛ حجم الإفصاح، وجودة الافصاح (وصفي – كمي – مالى)، وقابليته للقراءة Readability.

1-7 خطة الدراسة

في ضوء مشكلة الدراسة وأهدافها، سوف يتناول الباحثان العناصر التالية:

- المتغيرات البحثية؛ خلفية نظرية.
- جهود المنظمات المهنية لدعم الإفصاح عن الأمن السيبراني.
- تحليل الدراسات السابقة واشتقاق فروض البحث.
- الدراسة شبه التجريبية.
- الخلاصة والنتائج والتوصيات.
- مقترحات لدراسات مستقبلية.

2- المتغيرات البحثية؛ خلفية نظرية

2-1 الثالوث المظلم كسمات شخصية للمحاسبين: مفهومه وآثاره المحتملة على الإفصاح عن مخاطر الأمن السيبراني:

شهد العقد الأخير إهتماماً متزايداً بالسمات الشخصية المظلمة للموظفين الذين يسيئون استخدام وظائفهم مثل؛ الميكافيلية Machiavellianism والنرجسية Narcissism؛ والسيكوباتية Psychopathy، أو ما يُسمى بالثالوث المظلم The Dark Triad- تلك السمات تؤثر سلباً على الإنتاجية، والرضا الوظيفي، والمناخ الأخلاقي في منشآت الأعمال (Paulhus and Jones 2002; Amernic and Craig 2010; Jonason et al. 2012; Harrison et al. 2018).

في ضوء نظرية الصفوف العليا Upper Echelons Theory فإن للثالوث المظلم- كسمات شخصية للإدارة العليا-تأثير سلبي على القرارات التشغيلية والتمويلية والإستثمارية (Hambrick and Mason 1984)، وتلك القرارات المرتبطة بالإفصاح المحاسبي وإعداد التقارير المالية (Ramamoorti 2008;Cohen et al.2010; Ham et al. 2017; 2018; Mutschmann et al. 2021). في الاجتماع السنوي لجمعية المحاسبة الأمريكية عام 2011 حول القضايا الناشئة في الدراسات الأكاديمية حول الغش المحاسبي، أكد Brody et al. (2012) على أن منع الغش وإكتشافه في حالة حدوثه، يتطلب أن يتفهم المراجعون والجهات التنظيمية للمكون السلوكي للأفراد الذين يتورطون في تلك الممارسات.

ركز الباحثون في مجال الثالوث المظلم على النرجسية الإدارية كأحد جوانب الثالوث المظلم، نظراً لإمكانية ملاحظتها وقياسها في ضوء بعض المؤشرات التي لاقت قبولاً واسعاً من الباحثين مثل؛ حجم التوقيع، وحجم الصورة في التقارير السنوية، وتكرار ضمائر الشخص الأول "أنا" في المقابلات والمؤتمرات (Raskin and Shaw 1988; Chatterjee and Hambrick 2007; Ham et al. 2018)، الأمر الذي نتج عنه ظهور العديد من الدراسات العملية التي تفحص الآثار المحاسبية للنرجسية الإدارية دون إخضاع المديرين لإختبارات نفسية (Mutschmann et al. 2021).

أشار بعض الباحثين إلى تزايد ممارسات إدارة الأرباح مع تزايد النرجسية الإدارية (Olsen et al. 2014; Ham et al. 2017)، بل قد يتطور الأمر إلى الغش المحاسبي في بعض الأحيان (Ramamoorti 2008; Rijsenbilt and Commandeur 2013; Mutschmann et al. 2021). وفي مجال الإفصاح المحاسبي فقد أكد بعض الباحثين على إنخفاض مستوى الإفصاح الإختياري لدى المديرين النرجسيين (Mashayekh et al. 2021)، بينما يتزايد الإفصاح عن المبادرات الإجتماعية لدعم الجوانب النفسية للإدارة النرجسية، والذي رّبما يكون إفصاحاً إنتقائياً في الكثير من الأحيان (Lassoued and Khanchel 2022). كما أكد بعض الباحثين على تبني المديرون النرجسيون لنغمة الإفصاح الإيجابية عند الإفصاح عن الأرباح الحالية أو توقعات الأرباح المستقبلية (Ma 2015; Marquez-Illescas et al. 2019).

أما بخصوص الميكافيللية والسيكوباتية فلا توجد طرق مُعتبرة لقياس هذين المتغيرين سوى خضوع المديرين لإختبارات نفسية، الأمر قد يفسر ندرة البحوث المحاسبية في هذا المجال، وتُعد دراسة Mutschmann et al. (2021) أحد الدراسات الرائدة الحديثة التي تناولت الأبعاد الثلاثة للثالوث المظلم، وأثرها على الغش المحاسبي، وقد تم قياس الثالوث المظلم إستناداً للقياس غير المباشر للسمات الشخصية للمديرين [1].

يؤكد بعض الباحثين على وجود بعض الخصائص الفريدة لكل من الميكافيلليين والنرجسيين والسيكوباتيين، إلا أن هناك العديد من الخصائص المشتركة والتي من أهمها؛ أنها جميعاً تُشكل اضطراباً في الشخصية يتميز بالإزدواجية، والترويج الذاتي، والعدوانية، وبرودة العلاقات الشخصية، والميل للتلاعب بالآخرين، والشعور بالتفرد، وإنخفاض التعاطف، والقسوة وقلة الضمير، والإهتمام الكبير بالسمعة (Furnham et al. 2013; Maasberg et al. 2020; Mutschmann et al. 2021). إلا أن الميكافيلليين يتميزون بالرؤية الإستراتيجية الواضحة، كما يتميز النرجسيون بالشعور بالإستحقاق، والعظمة، والحاجة الدائمة لتعزيز الأنا Ego، بينما يتميز السيكوباتيون بالبحث الدائم عن الإثارة والتشويق، وإنخفاض القلق، والتهور وعدم القدرة على التحكم في الإنفعالات (Bailey 2015; Maasberg et al. 2020). لذلك تتزايد الممارسات الإحتيالية لدى الأفراد الميكافيلليين والنرجسيين والسيكوباتيين نظراً للسمات المشتركة بينهم، والتي تدفعهم للتصرف بشكل

[1] قام الباحثون في هذه الدراسة بتوجيه بعض الأسئلة للمحاسبين والمهنيين في أقسام المحاسبة في المنشآت المختلفة للتعرف على آرائهم الشخصية في المديرين، بدلاً من توجيه الأسئلة بشكل مباشر لهؤلاء المديرين (Mutschmann et al. 2021).

غير أخلاقي وخداع الآخرين (Cressey 1973; Dorminey et al. 2012; Trompeter et al. 2012; Bailey 2017; Harrison et al. 2018).

لذا فإننا نتوقع أن يتزايد مدى قبول المحاسبين ذوي السمات الشخصية المظلمة للإفصاح عن مخاطر الأمن السيبراني، كما نتوقع أن يعتمد هؤلاء المحاسبون على نغمة الإفصاح الإيجابية بشكل أكبر، نتيجة للسمات المشتركة بينهم والمرتبطة بالترويج الذاتي، والإهتمام بالسمعة. كما نتوقع تزايد إحتمالية توجههم نحو التلاعب بالإفصاح عن مخاطر الأمن السيبراني بشكل أكبر نتيجة السمات المرتبطة بالميل للتلاعب بالآخرين وإستغلالهم، والقسوة وإنعدام الضمير (Bailey 2015; Maasberg et al. 2020; Lassoued and Khanchel 2022).

يّلخص الجدول رقم (1) التالي السمات الشخصية للثالوث المظلم

جدول 1: السمات الشخصية للثالوث المظلم

الخصائص	الميكافيللية	النرجسية	السيكوباتية
الإزدواجية Duplicity	√	√	√
الترويج الذاتي Self-promotion	√	√	√
العدوانية Aggressiveness	√	√	√
برودة العلاقات الشخصية Interpersonal coldness	√	√	√
الميل للتلاعب بالآخرين وإستغلالهم Tendency to manipulate and exploit others	√	√	√
الشعور بالتفرد Sense of superiority	√	√	√
إنخفاض التعاطف Low empathy	√	√	√
القسوة وإنعدام الضمير Callousness/lack of conscience	√	√	√
الإهتمام بالسمعة Attention to reputation	√	√	√
النظرة الساخرة للعالم Cynical world view	√		
الرؤية الإستراتيجية Strategic calculation	√		
الشعور بالإستحقاق Sense of entitlement		√	
الشعور بالعظمة Sense of grandiosity		√	
تعزيز الأنا Ego-reinforcement		√	
البحث عن الإثارة Thrill-seeking			√
إنخفاض القلق Low anxiety			√
عدم القدرة على التحكم في الإنفعالات Lack of impulse control			√

المصدر: (Maasberg et al. 2020)

فـي ضـوء مـا تقـدم، يُلاحـظ أن الإزدواجيـة، والتـرويج الـذاتي، والعدوانيـة، وبـرودة العلاقـات الشخصـية، والميـل للتلاعـب بـالآخرين وإستغلالهم، والشـعور بـالتفرد، وإنخفـاض التعـاطف والقسـوة، والإهتمام بالسمعة هى سمات مشتركة بين الشخصيات الميكافيللية، والنرجسية، والسيكوباتية. بينما يتفرد الميكـافيلليون ببعض الخصـائص مثل، النظرة الساخرة للعالم، والرؤيـة الإستراتيجية. فـى حين يتفرد النرجسيون ببعض الخصـائص مثل، الشـعور بالاستحقاق، والشـعور بالعظمـة، وتعزيـز الأنـا. أخيراً، يتفرد السيكوباتيون ببعض الخصائص مثل، البحث عن الإثارة، وإنخفاض القلق، وعدم القدرة على التحكم فى الإنفعالات.

2-2 مخاطر الأمن السيبراني: مفهومها وأهمية الإفصاح عنها

تُشير مخاطر الأمن السيبراني إلى الخسائر المحتملة نتيجة الأحداث التي يقوم فيها فرد أو جهة غير مصرح لها بإختراق نظام المعلومات للمنشأة والوصول غير مصرح به إلى المعلومات المهمة وبنية إنتاجها (Frank et al. 2019)، لذا تنشأ مخاطر الأمن السيبراني نتيجة هجمات متعمدة أو أحداث غير متعمدة، تأخذ هذه الهجمات العديد من الأشكال، كما في حالة الوصول غير المصرح به إلى الأنظمة الرقمية لأغراض سرقة الأصول المالية، والفكرية، وغيرها من المعلومات الحساسة الخاصـة بالمنشـآت أو عملاءهـا، أو شـركاء الأعمـال الآخـرين، أو إفسـاد البيانـات، أو تعطيـل العمليات، ويمكن أيضاً تنفيذ تلك الهجمات بالإعتماد على هجمات الحرمان، التي تؤدي إلى رفض الخدمة على مواقع الويب للمنشأة. أيضاً قد يتم تنفيذ الهجمات من أفراد من خارج المنشأة أو من داخلها، لذا تتكبد المنشآت خسائر فادحة عند حدوث مثل هذه الهجمات (Dakin 2012).

تهـدف إدارة مخـاطر الأمـن السـيبراني إلـى الحـد مـن مخـاطر الهجمـات الضـارة علـى الفضـاء السيبراني ومشتملاته من البرامج وأجهزة الكمبيوتر، والشبكات، أو الوصول غير المصرح به للبيانات والمعلومـات لضـمان السـرية والنزاهـة، وإكتشـاف المتسـللين وإحبـاطهم، ويتضـمن ذلـك الأدوات المسـتخدمة لاكتشـاف عمليـات الاختـراق، وإيقـاف الفيروسـات، وحظـر الوصـول الضـار، وفـرض المصادقة، وتمكين الاتصالات المشفرة، لحماية البيئة السيبرانية، وأصول المنشأة، وحماية معلومات العملاء ذات الحساسية العالية، وأصحاب مصالح آخرين (Kemmerer 2003; Amoroso 2006; Perols 2019). يُمكن تعريـف إدارة مخـاطر الأمـن السيبراني علـى أنهـا مجموعـة مـن السياسـات والعمليات والضـوابط المصـممة لحمايـة المعلومـات، والأنظمـة مـن الأحـداث الأمنيـة التـي يمكـن أن تُعرِّض أهداف الأمن السيبراني للمنشأة للخطر. وكذلك اكتشاف والإستجابة للأحداث الأمنية والحد

من آثارها والتعافي من تلك الأحداث التي لم تستطع المنشأة منعها في التوقيت المناسب (AICPA 2017b, p. 207).

يمكن للمنشآت الحد من حالة عدم اليقين، وجعل الاستثمار في أسهمها أكثر جاذبية، من خلال توفير إفصاحات إضافية عن إدارة المخاطر (Deumes and Knechel 2008). وحيث أن الهجمات الإلكترونية مكلفة في الكثير من الأحيان، وتؤثر سلباً على الأداء المالي للمنشأة، ويعتبرها المستثمرون من أهم المخاطر التي تهدد نمو وبقاء المنشأة (SEC 2018). لذا، يقوم المستثمرون بدمج المعلومات عن المخاطر الإلكترونية في نماذج اتخاذ القرار (Ettredge and Richardson 2003; Wang et al. 2013; Frank et al. 2019).

الجهود التي تبذلها الإدارة لتقليل مخاطر الأمن السيبراني للمنشأة عادة لا يمكن ملاحظتها بشكل مباشر من قبل المستثمرين. لذا، يواجه المستثمرون درجة كبيرة من عدم اليقين فيما يتعلق بطبيعة ومدى وفعالية تلك الجهود عند اتخاذ قرارات الاستثمار في المنشآت. الأمر الذي يُشير إلى تزايد أهمية الإفصاح عن مخاطر الأمن السيبراني للمستثمرين وأصحاب المصالح، مع ضرورة وجود إطار تنظيمي يحكم عملية الإفصاح. لذا بدأت المنظمات المهنية تُولي إهتماماً متزايداً بالإفصاح عن مخاطر الأمن السيبراني منذ عام 2011 (SEC 2011). كما طوّر المعهد الأمريكي للمحاسبين القانونيين (AICPA) إطار عمل إختياري بالتعاون مع مجلس معايير المراجعة Auditing Standards Board، يهدف هذا الإطار إلى وضع أسس لإعداد تقارير إدارة مخاطر الأمن السيبراني (AICPA 2017a). يوفر هذا الإطار المفاهيمي وصفاً سردياً لبرنامج إدارة مخاطر الأمن السيبراني للمنشأة، والتأكيدات فيما يتعلق بما إذا كان هذا الوصف يتوافق مع إرشادات المعهد الأمريكي للمحاسبين القانونيين، وما إذا كانت الضوابط الموضوعة ضمن برنامج إدارة مخاطر الأمن السيبراني فعَّالة خلال الفترة المشمولة بالتقرير (AICPA 2017a). كما يهدف هذا الإطار إلى توفير لغة مشتركة يمكن لأصحاب المصالح استخدامها لتقييم موقف الأمن السيبراني للمنشأة وفعالية برنامج إدارة المخاطر الخاص بها (Yang et al. 2020).

في ضوء ما تقدم، يُلاحظ أن مخاطر الأمن السيبرانى أصبحت من المعلومات الضرورية لترشيد قرارات المستثمرين. كذلك فإن تنظيم هذا الإفصاح سوف يساهم في ترشيد القرارات الاستثمارية، وفى نفس الوقت سوف يُحسن أداء المنشأت في مجال إدارة مخاطر الأمن السيبرانى، حتى تتجنب الإفصاح عن أية معلومات سلبية في هذا المجال.

3- جهود المنظمات المهنية لدعم الإفصاح عن الأمن السيبراني

يُعد الإفصاح عن المخاطر أحد الموضوعات التي حازت على إهتمام المنظمات المهنية منذ الأزمة المالية العالمية 2008 (Heinle and Smith 2017)، وتُشير المخاطر بصفة عامة إلى الأحداث السلبية المحتملة مثل؛ الخسارة المالية، والاحتيال والسرقة، وفقدان السمعة، وفشل الأنظمة، والدعاوى القضائية (IFAC 1999, p.13). لذا يُعد الإفصاح عن مخاطر الأمن السيبراني أحد التوجهات الحديثة في الإفصاح عن المخاطر، نظراً لتزايد التهديدات التي تواجهها المنشآت في الآونة الأخيرة (Hilary et al. 2016). كذلك أصبح قراصنة الإنترنت والمهاجمين أكثر تطوراً مما يُعرِّض المنشآت لخسائر مالية وتشغيلية وقانونية، فضلاً عن فقدان السمعة وثقة العملاء والمستثمرين نتيجة حدوث تلك الإختراقات (SEC 2022).

لذا بدأت الجهات التنظيمية في الولايات المتحدة الأمريكية منذ عام 2011 بإصدار بعض التوصيات التي تؤكد على أهمية الإفصاح عن مخاطر الأمن السيبراني (Hilary et al. 2016)، حيث أصدرت هيئة تداول الأوراق المالية الأمريكية (SEC) عام 2011 إرشادات حول الإفصاح عن مخاطر الأمن السيبراني، وقد أشارت الهيئة إلى أنه عند تحليل مخاطر الأمن السيبراني لأغراض الإفصاح عنها، يجب على المنشآت المدرجة بالبورصة مراعاة ما يلي (SEC 2011):

- الحوادث الإلكترونية السابقة وشدة وتواتر تلك الحوادث.
- احتمالية وقوع الحوادث السيبرانية، والحجم الكمي، والنوعي لتلك المخاطر، بما في ذلك التكاليف المحتملة والعواقب الأخرى الناتجة عن اختلاس الأصول، والمعلومات الحساسة، وتلف البيانات، وتعطل العمليات.
- مدى كفاية الإجراءات الوقائية المتخذة لتقليل مخاطر الأمن السيبراني في سياق الصناعة التي تعمل فيها والمخاطر التي يتعرض لها الأمن السيبراني، بما في ذلك الهجمات بأنواعها المختلفة.
- كذلك أوضحت هيئة تداول الأوراق المالية الأمريكية (SEC 2011) أن الإفصاح قد يكون مناسباً في أقسام متعددة في القوائم المالية بما في ذلك القسم الخاص بعوامل الخطر Risk Factors، وتقرير مجلس الإدارة، ووصف الأعمال، والإجراءات القانونية، وإفصاحات البيانات المالية مثل؛ تكاليف الوقاية المادية، أو الخسائر المتكبدة. يشير Masterson (2015) إلى أن إرشادات الهيئة تشجع المنشآت المسجلة بالبورصة على تعزيز الإفصاح عن المخاطر والحوادث السيبرانية بعد إصدار تلك الإرشادات.

كما لاقت متطلبات الإفصاح عن مخاطر الأمن السيبراني–الصادرة عن هيئة تداول الأوراق المالية الأمريكية (SEC)– إهتمام كبير من الباحثين والمنظمين وتم الترويج لها من قبل أعضاء مجلس الشيوخ الأمريكي، والمهنيين، والمديرين التنفيذيين، باعتبارها تحولاً رئيساً له عواقب وخيمة في حالة إهماله وعدم تقديم إفصاحات عنه. على سبيل المثال، صرح السناتور John Rockefeller: "لقد سرق مجرمو الإنترنت الملكية الفكرية التي تبلغ قيمتها مليارات الدولارات، وتم إبقاء المستثمرين في الظلام التام، نتوقع أن تُغير متطلبات الإفصاح كل شيء، حيث سيتمكن المشاركين في السوق من تقييم المنشآت جزئياً بناءً على قدرتها على الحفاظ على أمان شبكاتها، نريد حالة من الشفافية لحماية المستثمرين والأسواق" (Hilary et al. 2016, p.8).

في عام 2017 أصدر المعهد الأمريكي للمحاسبين القانونيين (AICPA) إطار متكامل لإعداد تقارير مخاطر الأمن السيبراني وسُبل إدارتها. يتمثل الهدف الرئيس لهذا الإطار في توفير معلومات تقلل من حالة عدم اليقين بشأن قدرة المنشأة على إدارة مخاطر الأمن السيبراني، وبالتالي جعل الاستثمارات في المنشآت التي تُدير هذه المخاطر بشكل جيد أكثر جاذبية (Frank et al. 2019). يشتمل الإطار الذي قدمه المعهد الأمريكي للمحاسبين القانونيين على إعداد تقرير يشتمل على ثلاثة أقسام (Yang et al. 2020): **القسم الأول؛** يتضمن وصفاً سردياً لمخاطر الأمن السيبراني وسُبل إدارتها، ويشتمل هذا القسم على تسعة عناصر وهي؛ [1] طبيعة أعمال المنشأة وعملياتها الرئيسة. [2] طبيعة المعلومات المُعرضة للخطر. [3] الأهداف المتوقعة من برنامج إدارة مخاطر الأمن السيبراني. [4] العوامل التي تؤثر على المخاطر الحتمية للأمن السيبراني مثل التكنولوجيا المستخدمة، وأنواع الإتصالات ومقدمي الخدمة، والتغييرات الجوهرية في البيئة التكنولوجية والتنظيمية خلال الفترة. [5] هيكل حوكمة مخاطر الأمن السيبراني. [6] عملية تقييم مخاطر الأمن السيبراني. [7] اتصالات الأمن السيبراني وجودة معلومات الأمن السيبراني. [8] ضوابط الرقابة على برنامج إدارة مخاطر الأمن السيبراني. [9] عمليات مراقبة الأمن السيبراني. **القسم الثاني؛** يشتمل على تأكيد الإدارة بأن إعداد القسم الأول يتوافق مع المعايير التي وضعها المعهد الأمريكي للمحاسبين القانونيين في هذا الشأن، كما تؤكد الإدارة على فعالية أنظمة الرقابة على مخاطر الأمن السيبراني، **القسم الثالث:** رأي مراقب الحسابات بشأن تقرير إدارة مخاطر الأمن السيبراني للمنشأة، وفعالية الضوابط المطبقة لتلبية أهداف الأمن السيبراني (AICPA 2017a)

.

تؤكد Susan Coffey نائب الرئيس التنفيذي للمعهد الأمريكي للمحاسبين القانونيين، على أهمية وجود إطار موحد للإفصاح عن مخاطر الأمن السيبراني، فقد أوضحت أن الإطار الموحد للإفصاح الذي تم تطويره سيكون بمثابة خطوة حاسمة لتحقيق الاتساق في الإفصاح عن مخاطر الأمن السيبراني، كذلك ستؤدي هذه المعلومات جنباً إلى جنب مع رأي المراجع حول فعّالية جهود الإدارة، إلى زيادة ثقة أصحاب المصالح في جهود إدارة مخاطر الأمن السيبراني (AICPA 2017c).

في عام 2019 صُنفت المخاطر الإلكترونية كواحدة من أهم المخاطر التي تواجه المنشآت في الولايات المتحدة، وكندا، وأوروبا (World Economic Forum 2019). نظراً لخطورة تلك الهجمات وأضرارها المحتملة على المستثمرين والجمهور، لذا فإنه من المتوقع أن يظل مجلس الإدارة يقظاً بإستمرار وأن يتبنى نهجاً أكثر شمولاً لإدارة مخاطر الأمن السيبراني (Abraham et al. 2019;SEC 2018)، كذلك يجب أن تدعم أطراف حوكمة الشركات عملية الإفصاح عن المخاطر الجوهرية التي قد تؤثر على عملية صنع القرار لدى المستثمرين، وسُبل مواجهة تلك المخاطر (Deumes and Knechel 2008)، فضلاً عن تقرير التأكيد المستقل لهذه المعلومات (Frank et al. 2019).

وفي كندا، طوَّرت هيئة تداول الأوراق المالية الكندية The Canadian Securities Administrators (CSA) إرشادات للإفصاح عن مخاطر الأمن السيبراني عام 2017، تتضمن تلك الإرشادات الإفصاح عن الآثار المحتملة للهجمات الإلكترونية، والإفصاح عن الحوكمة ودورها في الحد من تلك المخاطر، كما إتخذت العديد من الدول العربية خطوات إيجابية لتعزيز الأمن السيبراني لدى المنشآت، حيث أصدرت هيئة سوق المال السعودية الدليل الإسترشادي للأمن السيبراني لمؤسسات السوق المالية، والذي يهدف إلى إرساء الضوابط الخاصة بالأمن السيبراني في المنشآت السعودية، والتي تُساعدها على الإدارة الجيدة لمخاطر الأمن السيبراني، من خلال تبني أفضل الممارسات الدولية وتشريعات الأمن السيبراني الصادرة في السعودية (هيئة السوق المالية السعودية 2019).

كما نص الدستور المصري الصادر عام 2014 على أن ""أمن الفضاء المعلوماتي جزء أساسي من منظومة الإقتصاد والأمن القومي، وتلتزم الدولة بإتخاذ التدابير اللازمة للحفاظ عليه على النحو الذي ينظمه القانون"، لذا تم إنشاء المجلس الأعلى لتأمين البنى التحتية للاتصالات والمعلومات، وبرئاسة وزير الاتصالات، وبتبعية مباشرة لرئاسة مجلس الوزراء، حيث تم تكليفه بوضع

الاستراتيجية الوطنية للأمن السيبراني (2017-2021)، حيث تهدف تلك الاستراتيجية إلى تأمين البنى التحتية للاتصالات والمعلومات بشكل متكامل، لتوفير البيئة الآمنة لمختلف القطاعات لتقديم الخدمات الالكترونية المتكاملة، إلا أنه حتى الآن لم يصدر أية إرشادات عن هيئة سوق المال أو البورصة المصرية أو أية جهة أخرى لتنظيم الإفصاح عن الأمن السيبراني في مصر.

في ضوء ما تقدم، يُلاحظ الباحثان تزايد إهتمام المنظمات المهنية في الدول المتقدمة بالإفصاح عن مخاطر الأمن السيبراني، وصدور العديد من الإرشادات والتوصيات لدعم هذا الإفصاح. في حين لم يحظى هذا الموضوع بنفس الإهتمام في الدول النامية. كما يُلاحظ عدم وجود توجه صريح في معايير المحاسبة الدولية لدعم الإفصاح عن مخاطر الأمن السيبرانى وما زالت تتم عمليات الإفصاح في ضوء القواعد الحالية كجزء من الإفصاح المالي عند الإفصاح عن خسائر الحوادث السيبرانية، أو في إطار الإفصاح الإختياري، ومن وجهة نظرنا فإنه قد آن الأوان لتبني مجلس معايير المحاسبة الدولية (IASB) قواعد خاصة للإفصاح عن مخاطر الأمن السيبراني بما يساهم فى توفير معلومات مفيدة لمتخذى القرارات، ويساهم فى تحسين فعالية إدارة مخاطر الأمن السيبراني لدى المنشآت.

4- تحليل الدراسات السابقة واشتقاق فروض البحث

4-1 الميكافيللية Machiavellianism:

تُعد الميكافيللية سمة شخصية يميل أفرادها لعدم الثقة بالآخرين، والانخراط في التلاعب غير الأخلاقي، والسعي للتحكم والسيطرة على الآخرين، ولديهم رغبة مُلحة في تحقيق مكانة مرموقة (Dahling et al. 2009)، كما أنهم أكثر اهتماماً بأنفسهم وأكثر إنتهازية (Gunnthorsdottir et al. 2002)، ولا يمكنهم الإنخراط في ولاءات معينة (محمد 2021)، إلا بقدر ما يحقق رؤيتهم الاستراتيجية (Jones and Paulhus 2011). لذا فإنه من المرجح أن تمارس الشخصيات الميكافيللية الغش، وتكون قادرة على تبرير سلوكها (Cooper and Peterson 1980; Fehr et al. 1992). إن استغلال الآخرين يتجلى بوضوح في الشخصيات الميكافيللية، كما أن لديهم قدرة إستثنائية على التلاعب بالآخرين (Dahling et al.2009)، لتحقيق مصالحهم الخاصة (Christie and Geis 1970). إنهم دوماً غير راضين عن وضعهم المهني، ويعتقدون أن التلاعب هو مفتاح النجاح في الحياة (Paulhus and Jones 2015)، كما تتزايد إحتمالية سرقتهم لجهود الآخرين (Fehr et al. 1992)، نتيجة إيمانهم بأن الآخرين ساذجون وحمقى، فضلاً عما يحملونه من

وجهات نظر ساخرة تجاه الآخرين، وإعتقادهم بأن التلاعب طريقة صالحة ومفيدة لتحقيق أهدافهم الشخصية (Harrison et al. 2018).

كذلك أكد Murphy (2012) في دراسته التجريبية على أن الأفراد الذين حصلوا على درجات عالية في إختبار الميكافيللية يميلون للتلاعب بدرجة أكبر وينخفض لديهم الشعور بالذنب، لذا تُحفز الميكافيللية الأفراد على التصرف بشكل غير أخلاقي، ويفترضون غالباً أن الآخرين سيتخذون نفس القرارات غير الأخلاقية، ولا مانع لديهم من تغيير الحقائق لخداع الآخرين (Jones and Paulhus 2011; Harrison et al. 2018). لذا فإنه من المتوقع أن يقوم الميكافيلليون بممارسة الغش والإحتيال المالي بشكل أكبر (Shafer and Wang 2011; Vladu 2013; Harrison et al. 2018; Utami et al. 2019).

وبناءً على ذلك؛ نتوقع أن لا يُبدي الميكافيلليون في البنوك العاملة في مصر أي رفض للإفصاح عن مخاطر الأمن السيبراني، بل نتوقع قبولهم لهذا النوع من الإفصاح، لقدرتهم غير العادية على إستغلال كل شيئ لتحقيق رؤيتهم الاستراتيجية، حيث يمكنهم الإعتماد بشكل أكبر على نغمة الإفصاح الإيجابية والتي تُطمئن المستثمرين، والتوجه نحو التلاعب والتحايل لإخفاء المعلومات السلبية قدر الإمكان، كما في حالة تجنب الإفصاح عن الخسائر الفعلية نتيجة محاولات الإختراق السابقة، أو الخسائر المحتملة نتيجة الإختراقات المتوقعة، في ضوء ما تقدم فإنه سيتم صياغة الفرض الرئيس الأول للدراسة كما يلي:

H1: يوجد تأثير إيجابي معنوي للميكافيللية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على اتجاهاتهم نحو الإفصاح عن مخاطر الأمن السيبراني، وينبثق عن هذا الفرض مجموعة من الفروض الفرعية التالية:

- H11: يوجد تأثير إيجابي معنوي للميكافيللية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على مدى قبولهم للإفصاح عن مخاطر الأمن السيبراني.
- H12: يوجد تأثير إيجابي معنوي للميكافيللية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على نغمة الإفصاح الإيجابية عن مخاطر الأمن السيبراني.
- H13: يوجد تأثير إيجابي معنوي للميكافيللية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على إحتمالية التلاعب بالمعلومات المرتبطة بمخاطر الأمن السيبراني.

2-4 النرجسية Narcissism

يُمكن الإستدلال على النرجسية بخمسة أو أكثر من المظاهر التالية (جمعية الطب النفسي الأمريكي2004، ص 152): [1] الشعور بأهمية الذات. [2] الإستغراق في خيالات النجاح اللامحدود أو القوة أو التألق والجمال. [3] الإعتقاد بالتميز والتفرد وإيمانه بأنه يجب أن يُصاحب من قبل شخصيات مهمة. [4] يتطلب تقديراً مبالغ فيه. [5] الشعور بالإستحقاق وتوقع معاملة خاصة من الآخرين. [6] إستغلال الآخرين لتحقيق أهدافه الخاصة. [7] الإفتقار إلى التعاطف. [8] يحسد الآخرين، أو يعتقد أنهم يحملون مشاعر الحسد تجاهه. [9] يُبدي سلوكيات متعالية ومتعجرفة.

لذا يبدو أن العلاقات الشخصية للنرجسيين قائمة على الإستعراض وجذب الإنتباه Exhibitionism، ومحاولة استغلال الآخرين (Campbell et al.2004). كما أنهم يميلون للتورط في السلوكيات غير الأخلاقية، مثل الغش على شركائهم (Buss and Shackelford 1997)، والغش لتحسين أدائهم الأكاديمي (Menon and Sharland 2011). وبالتالي، قد تسهل سمات الشخصية النرجسية السلوك الاحتيالي من خلال إستغلال الفرص المتاحة والتبرير العقلي. لذا تنخفض النزاهة الشخصية مع تزايد النرجسية لدى الأفراد، وعلى مستوى منشآت الأعمال فإن النرجسية الإدارية المرتفعة تخلق بيئات عمل مدمرة (Schlenker 2008; O'Reilly et al. 2013; Domino et al. 2015). الدراسات الحديثة في سيكولوجية الإدارة التنفيذية تؤكد على إنخفاض جودة القرارات التنظيمية في المنشآت مع تزايد النرجسية الإدارية، وهو ما يؤثر سلباً على العديد من أصحاب المصالح (Chatterjee and Hambrick 2007;Olsen and Stekelberg 2016).

توثق الأدبيات المحاسبية وجود تأثير سلبي للنرجسية الإدارية على فعالية نظم الرقابة الداخلية (Chatterjee and Pollock 2016; Young et al. 2014)، وإنخفاض جودة التقارير المالية (Ham et al. 2017; Capalbo et al. 2018; Buchholz et al. 2019)، والتورط في ممارسات الغش المحاسبي (Ramamoorti 2008; Rijsenbilt and Commandeur 2013; Mutschmann et al. 2021)، وفي مجال الإفصاح المحاسبي يؤكد Ma (2015) على إنخفاض إحتمالية إصدار توقعات للأرباح من المديرين النرجسيين، كما ترتبط النرجسية الإدارية سلباً مع دقة تلك التنبؤات، كما يؤكد Marquez-Illescas et al. (2019) على أن المديرين التنفيذيين النرجسيين يميلون إلى تعزيز صورتهم الذاتية المبالغ فيها من خلال الإعتماد على النغمة الإيجابية عند الإعلان عن الأرباح المتفائلة. كذلك لاحظ (Mashayekh et al. 2021) إنخفاض

مستوى الإفصاح الإختياري مع تزايد النرجسية الإدارية. كما أكد Lassoued and Khanchel (2022) على تزايد مستوى الإفصاح عن المسئولية الإجتماعية مع تزايد النرجسية الإدارية لدعم صورتهم الذاتية الرائعة. إنهم يميلون إلى الإفصاح عن المعلومات التي تُظهر الاحترام لحقوق المساهمين، ومكافحة الرشوة، ومكافحة الفساد، حتى لو تطلب ذلك اللجوء إلى الإفصاح الانتقائي لإخفاء ممارساتهم غير الأخلاقية.

لذا فإننا نتوقع قبول النرجسيون في البنوك العاملة في مصر للإفصاح عن مخاطر الأمن السيبراني، وخاصة الجوانب الإيجابية في هذا النوع من الإفصاح للحصول على الثناء المتكرر والإعجاب (Rijsenbilt and Commandeur 2013). وفي حالة تنظيم هذا النوع من الإفصاح؛ فإنه من المتوقع أن يتجه النرجسيون للإفصاح عن الجوانب الإيجابية التي تعزز لديهم الشعور بالعظمة وتُطمئن المستثمرين، معتمدين في ذلك على النغمة الإيجابية في الإفصاح، كما أنه من المتوقع أن يتجه النرجسيون للتحايل لإخفاء المعلومات السلبية، كما في حالة تجنب الإفصاح عن الخسائر الفعلية نتيجة محاولات الإختراق السابقة، أو الخسائر المحتملة نتيجة الإختراقات المتوقعة، في ضوء ما تقدم فإنه سيتم صياغة الفرض الرئيس الثاني للدراسة كما يلي:

H2: يوجد تأثير إيجابي معنوي للنرجسية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على اتجاهاتهم نحو الإفصاح عن مخاطر الأمن السيبراني، وينبثق عن هذا الفرض مجموعة من الفروض الفرعية التالية:

- H21: يوجد تأثير إيجابي معنوي للنرجسية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على مدى قبولهم للإفصاح عن مخاطر الأمن السيبراني.
- H22: يوجد تأثير إيجابي معنوي للنرجسية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على نغمة الإفصاح الإيجابية عن مخاطر الأمن السيبراني.
- H23: يوجد تأثير إيجابي معنوي للنرجسية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على إحتمالية التلاعب بالمعلومات المرتبطة بمخاطر الأمن السيبراني.

4-3 السيكوباتية Psychopathy

تُعد السيكوباتية أكثر السمات السلبية للثالوث المظلم مقارنة بالميكافيللية والنرجسية (Paulhus and Williams 2002; Rauthmann and Kolar 2012; Mutschmann et al. 2021). ويمكن تعريفها على أنها اضطراب في الشخصية له بعدين وهما؛ [1] **البعد الرئيس:** يتضمن الميل للكذب، وعدم الندم، والقسوة، والتلاعب، وإنخفاض التعاطف، وإنخفاض القلق، وعادة ما يتم تسهيل

هذه الميول من خلال السحر السطحي Superficial Charm؛ والذي يعني لجوء الفرد السيكوباتي لقول الأشياء التي يستقبلها الآخرون جيداً، وليس ما يعتقده هو، أو يريده بالفعل، إنهم يخبرون الآخرين بما يريدون سماعه. [2] **البعد الثانوي:** يشتمل على الاندفاع وعدم تحمل الإحباط وسرعة الانفعال وعدم وجود أهداف طويلة المدى (Ray and Ray 1982; Fehr et al. 1992; Babiak and Hare 2006; Bailey 2015; 2017).

لذا فإن السيكوباتيين يتورطون في العديد من السلوكيات المعادية للمجتمع (Hare 1991; Fehr et al. 1992; Patrick 2007). إنهم يتخلون عن كل شيئ حتى الأصدقاء والعائلة (Jones and Paulhus 2014). كما أنهم لا يستجيبون بشكل جيد للعلاج، إنهم يعرفون الصواب من الخطأ، لكن لا يٌبالون بذلك، وليس لديهم الدافع ليكونوا أخلاقيون أو يُنظر إليهم من هذا المنظور (Glenn et al. 2010; Bailey 2017). كذلك فإنهم يبحثون دائماً عن الإثارة (Hare 1985; Lilienfeld and Andrews 1996).

على مستوى منشآت الأعمال، ترتبط السيكوباتية بالاختلال الوظيفي (Jones and Paulhus 2011)، إذ تؤثر السمات الشخصية للمديرين السيكوباتيين على الجوانب الثلاثة لمثلث الغش في المناصب الإدارية العليا (Bailey 2017)، إنهم يُشكلون أكبر تهديد لأخلاقيات العمل (Marshall et al. 2015). وأكثر استعداداً للاحتيال على المنشأة التي توظفهم للحصول على أجر أو ترقية أعلى (Clarke 2005).

إستناداً للسحر السطحي Superficial Charm للسيكوباتيين فإنه من المتوقع أن يقبلوا الإفصاح عن مخاطر الأمن السيبراني، إنهم يخبرون الآخرون بما يريدون سماعه، وليس ما يعتقدونه بالفعل (Bailey 2017). كما يؤكد Kirkman (2005) على أن الاحتيال هو الجريمة المتكررة بين الأفراد ذوي السمات السيكوباتية، لذا فإنه من المتوقع أن يكون لها آثار كبيرة على الاحتيال والسلوك غير الأخلاقي من قبل المحاسبين والمراجعين (Bailey 2017; Harrison et al. 2018)، نتيجة إنعدام الضمير، وإنخفاض القلق (Paulhus and Williams 2002).

لذا عند تنظيم هذا النوع من الإفصاح فإنه من المتوقع أن يتجه السيكوباتيون فى البنوك العاملة في مصر للإفصاح عن الجوانب الإيجابية والتي تُطمئن المستثمرين، إستناداً لنغمة الإفصاح الإيجابية، كذلك من المتوقع أن يتجهون للتحايل من أجل عدم الإفصاح عن المعلومات السلبية، كما في حالة تجنب الإفصاح عن الخسائر الفعلية نتيجة محاولات الإختراق السابقة، أو الخسائر

المحتملة نتيجة الإختراقات المتوقعة. في ضوء ما تقدم فإنه سيتم صياغة الفرض الرئيس الثالث للدراسة كما يلي:

H3: يوجد تأثير إيجابي معنوي للسيكوباتية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على اتجاهاتهم نحو الإفصاح عن مخاطر الأمن السيبراني، وينبثق عن هذا الفرض مجموعة من الفروض الفرعية التالية:

-H31: يوجد تأثير إيجابي معنوي للسيكوباتية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على مدى قبولهم للإفصاح عن مخاطر الأمن السيبراني.

-H32: يوجد تأثير إيجابي معنوي للسيكوباتية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على نغمة الإفصاح الإيجابية عن مخاطر الأمن السيبراني.

-H33: يوجد تأثير إيجابي معنوي للسيكوباتية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على إحتمالية التلاعب بالمعلومات المرتبطة بمخاطر الأمن السيبراني.

5- الدراسة شبه التجريبية

قام الباحثان بإجراء دراسة شبه تجريبية- إستناداً لمنهجية Johnson et al. (2013)- على عينة من المحاسبين العاملين فى عينة من كبرى البنوك في جمهورية مصر العربية (بمختلف مسمياتهم الوظيفية)، كأحد أهم القطاعات تأثُراً بمخاطر الأمن السيبراني. وتهدف هذه الدراسة إلى استكشاف أثر الثالوث المظلم كسمات شخصية للمحاسبين على اتجاهاتهم نحو الإفصاح عن مخاطر الأمن السيبراني. وقد قام الباحثان بصياغة حالة افتراضية لأحد البنوك التى تعرضت لمحاولة إختراق من مهاجمين (قراصنة)؛ وقد طُلب من المستقصي منهم قراءة الحالة بشكل جيد قبل الإجابة عن الأسئلة المرفقة بها، حيث تم صياغة المجموعة الأولى من الأسئلة لقياس اتجاهات المحاسبين نحو الإفصاح عن مخاطر الأمن السيبراني، والمجموعة الثانية لقياس الثالوث المظلم في شخصية المحاسبين.

5-1 عينة الدراسة

اعتمد الباحثان على عينة من المحاسبين العاملين ببعض البنوك الكبرى فى جمهورية مصر العربية، ويوضح الجدول رقم (2) التالى عدد القوائم السليمة المستلمة من كل بنك:

جدول 2: يوضح حجم العينة النهائية

اسم البنك	عدد القوائم السليمة المستلمة	النسبة
البنك الأهلى المصرى	27	%26.73
بنك مصر	25	%24.75
البنك التجاري الدولي	26	%25.74
بنك الإسكندرية	23	%22.78
الإجمالى	101	%100

5-2 تصميم الدراسة

اعتمد الباحثان على الاستبانة كأداة لجمع البيانات، وهى أداة شائعة فى هذا النوع من الدراسات التى ترصد الاتجاهات والمواقف عند المبحوثين (Bailey 2019; Mutschmann et al. 2021). وقد اشتملت الاستبانة على أربعة أقسام، **القسم الأول:** ويتضمن بعض البيانات العامة (الإسم، العمر، النوع، المؤهل العلمى، وعدد سنوات الخبرة). **القسم الثانى:** إشتمل على أهم المصطلحات الواردة في الحالة الإفتراضية. **القسم الثالث:** إشتمل على حالة افتراضية لأحد البنوك التى تعرضت لمحاولة إختراق من بعض المهاجمين (قراصنة الإنترنت). **القسم الرابع:** إشتمل على مجموعتين من الأسئلة وهى؛ **المجموعة الأولى:** إشتملت على مجموعة من الأسئلة لقياس متغيرات الإفصاح والتي تتمثل في؛ مدى قبول المحاسبين للإفصاح عن مخاطر الأمن السيبرانى، ومدى اعتماد المحاسبين على النغمة الإيجابية للإفصاح عن مخاطر الأمن السيبراني، وأخيراً التلاعب المحتمل فى هذا الإفصاح. **المجموعة الثانية:** إشتملت على مجموعة من الأسئلة لقياس السمات الشخصية المظلمة للمحاسبين، والتي تتمثل في الميكافيللية، والنرجسية، والسيكوباتية (Jones and Paulhus 2014)، وقد إشتملت هذه المجموعة على 27 سؤال بواقع 9 أسئلة لكل بُعد من أبعاد الثالوث المظلم. وقد تم تحكيم الإستبانة من قبل أربعة من أساتذة المحاسبة والمراجعة ذوي الإهتمام بالإفصاح المحاسبي، وقد تم إجراء تعديلات طفيفة عليها –قبل توزيعها على المحاسبين– في ضوء ما ورد إلينا من تعليقات من المحكمين، بعد ذلك تم تنظيم الاستبانة وتوزيعها إلكترونياً على عينة الدراسة.

5-3 صياغة النماذج البحثية لاختبار الفروض

تم الاعتماد على نماذج الإنحدار التالية لاختبار فروض الدراسة وذلك على النحو التالى:

5-3-1 نموذج اختبار الفرض الرئيس الأول H1

الفرض الرئيس الأول: يوجد تأثير إيجابي معنوي للميكافيللية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على اتجاهاتهم نحو الإفصاح عن مخاطر الأمن السيبراني. وينبثق عن هذا الفرض مجموعة من الفروض الفرعية التالية:

H11: يوجد تأثير إيجابي معنوي للميكافيللية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على مدى قبولهم للإفصاح عن مخاطر الأمن السيبراني، ولاختبار هذا الفرض **(H11)**، سيتم الاعتماد على نموذج الانحدار رقم (1) التالي:

$$DISC\_ACCEPT = B_0 + B_1\ MACH + B_2\ Gender + B_3\ Age + B_4\ Qualification + B_5\ Expert + \varepsilon\ (1)$$

H12: يوجد تأثير إيجابي معنوي للميكافيللية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على نغمة الإفصاح الإيجابية عن مخاطر الأمن السيبراني، ولاختبار هذا الفرض **(H12)**، سيتم الاعتماد على نموذج الانحدار رقم (2) التالي:

$$DISC\_TONE = B_0 + B_1\ MACH + B_2\ Gender + B_3\ Age + B_4\ Qualification + B_5\ Expert + \varepsilon\ (2)$$

H13: يوجد تأثير إيجابي معنوي للميكافيللية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على إحتمالية التلاعب بالمعلومات المرتبطة بمخاطر الأمن السيبراني، ولاختبار هذا الفرض **(H13)**، تم الاعتماد على نموذج الانحدار رقم (3) التالي:

$$DISC\_MANIP = B_0 + B_1\ MACH + B_2\ Gender + B_3\ Age + B_4\ Qualification + B_5\ Expert + \varepsilon\ (3)$$

5-3-2 نموذج اختبار الفرض الرئيس الثانى H2

الفرض الرئيس الثاني: يوجد تأثير إيجابي معنوي للنرجسية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على اتجاهاتهم نحو الإفصاح عن مخاطر الأمن السيبراني. وينبثق عن هذا الفرض مجموعة من الفروض الفرعية التالية:

H21: يوجد تأثير إيجابي معنوي للنرجسية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على مدى قبولهم للإفصاح عن مخاطر الأمن السيبراني. ولاختبار هذا الفرض **(H21)**، سيتم الاعتماد على نموذج الانحدار رقم (4) التالي:

$$DISC\_ACCEPT = B_0 + B_1\ NAR + B_2\ Gender + B_3\ Age + B_4\ Qualification + B_5\ Expert + \varepsilon \quad (4)$$

H22: يوجد تأثير إيجابي معنوي للنرجسية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على نغمة الإفصاح الإيجابية عن مخاطر الأمن السيبراني. ولاختبار هذا الفرض **(H22)**، سيتم الاعتماد على نموذج الانحدار رقم (5) التالي:

$$DISC\_TONE = B_0 + B_1\ NAR + B_2\ Genderit + B_3\ Age + B_4\ Qualification + B_5\ Expert + \varepsilon \ (5)$$

H23: يوجد تأثير إيجابي معنوي للنرجسية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على إحتمالية التلاعب بالمعلومات المرتبطة بمخاطر الأمن السيبراني. ولاختبار هذا الفرض **(H23)**، سيتم الاعتماد على نموذج الانحدار رقم (6) التالي:

$$DISC\_MANIP = B_0 + B_1\ NAR + B_2\ Gender + B_3\ Age + B_4\ Qualification + B_5\ Expert + \varepsilon \ (6)$$

5-3-3 نموذج اختبار الفرض الرئيس الثالث H3

الفرض الرئيس الثالث: يوجد تأثير إيجابي معنوي للسيكوباتية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على اتجاهاتهم نحو الإفصاح عن مخاطر الأمن السيبراني. وينبثق عن هذا الفرض مجموعة من الفروض الفرعية التالية:

H31: يوجد تأثير إيجابي معنوي للسيكوباتية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على مدى قبولهم للإفصاح عن مخاطر الأمن السيبراني. ولاختبار هذا الفرض **(H31)**، سيتم الاعتماد على نموذج الانحدار رقم (7) التالي:

$$DISC\_ACCEPT = B_0 + B_1\ PSYC + B_2\ Gender + B_3\ Age + B_4\ Qualification + B_5\ Expert + \varepsilon \ (7)$$

H32: يوجد تأثير إيجابي معنوي للسيكوباتية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على النغمة الإيجابية للإفصاح عن مخاطر الأمن السيبراني. ولاختبار هذا الفرض **(H32)**، سيتم الاعتماد على نموذج الانحدار رقم (8) التالي:

$$DISC\_TONE= B_0 + B_1\ PSYC+ B_2\ Gender + B_3\ Age + B_4\ Qualification + B_5\ Expert + \varepsilon \quad (8)$$

H33: يوجد تأثير إيجابي معنوي للسيكوباتية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على إحتمالية التلاعب بالمعلومات المرتبطة بمخاطر الأمن السيبراني. ولاختبار هذا الفرض **(H33)**، سيتم الاعتماد على نموذج الانحدار رقم (9) التالي:

$$DISC\_MANIP= B_0 + B_1\ PSYC+ B_2\ Gender + B_3\ Age + B_4\ Qualification + B_5\ Expert + \varepsilon \quad (9)$$

حيث إن:

- **DISC_ACCEPT:** مدى قبول المستقصى منه الإفصاح عن مخاطر الأمن السيبرانى، وسيتم قياسه من خلال متوسط إجابات المستقصى منه عن الأسئلة (Q1-Q3) في المجموعة الأولى (انظر ملحق رقم1).
- **DISC_TONE:** توجه المستقصى منه نحو الإعتماد على النغمة الإيجابية للإفصاح عند تنظيم الإفصاح عن مخاطر الأمن السيبراني، وسيتم قياسه من خلال متوسط إجابات المستقصى منه عن الأسئلة (Q4-Q6) في المجموعة الأولى (أنظر ملحق رقم1).
- **DISC_MANIP:** توجه المستقصى منه نحو التلاعب بالمعلومات المرتبطة بمخاطر الأمن السيبراني، وسيتم قياسه من خلال متوسط إجابات المستقصى منه عن الأسئلة (Q7-Q9) في المجموعة الأولى (أنظر ملحق رقم 1).
- **MACH:** مستوى الميكافيللية لدى المستقصى منه، وسيتم قياسه من خلال متوسط إجابات المستقصى منه عن الأسئلة (Q1-Q9) في المجموعة الثانية (أنظر ملحق رقم 1).
- **NAR:** مستوى النرجسية لدى المستقصى منه، وسيتم قياسه من خلال متوسط إجابات المستقصى منه عن الأسئلة (Q10-Q18) في المجموعة الثانية (أنظر ملحق رقم 1).
- **PSYC:** مستوى السيكوباتية لدى المستقصى منه، وسيتم قياسه من خلال متوسط إجابات المستقصى منه عن الأسئلة (Q19-Q27) في المجموعة الثانية (أنظر ملحق رقم 1).
- **Gender:** متغير رقابى، يأخذ القيمة (1) إذا كان المستقصى منه ذكر، والقيمة (2) إذا كان المستقصى منه أنثى.
- **Age:** متغير رقابى، يعبر عن عمر المستقصى منه.
- **Qualification:** متغير رقابى، يعبر عن المؤهل العلمى للمستقصى منه.
- **Expert:** متغير رقابى، يعبر عن عدد سنوات الخبرة التى يمتلكها للمستقصى منه.

5-4 خصائص العينة

يوضح الجدول رقم (3) التالى الخصائص الديموجرافية للعينة النهائية:

جدول 3: الخصائص الديموجرافية للعينة النهائية

	الفئة	العدد	النسبة
العمر	أقل من 30 سنة	12	%11.9
	30-39 سنة	72	%71.3
	40-49 سنة	11	%10.9
	أكثر من 50 سنة	6	%5.9
	الإجمالى	101	%100
	المؤهل	**العدد**	**النسبة**
المؤهل العلمى	بكالوريوس	50	%49.5
	ماجستير	33	%32.7
	دكتوراه	18	%17.8
	الإجمالى	101	%100
	النوع	**العدد**	**النسبة**
النوع	ذكر	95	%94.1
	أنثي	6	%5.9
	الإجمالى	101	%100
	سنوات الخبرة	**العدد**	**النسبة**
سنوات الخبرة	أقل من 5 سنوات	12	%11.9
	5- 10 سنوات	16	%15.8
	11-15 سنة	57	%56.4
	16-20 سنة	5	%5
	أكثر من 20 سنة	11	%10.9
	الإجمالى	101	%100

في ضوء الجدول رقم (3) السابق يُلاحظ أن الفئة العمرية للعينة تركزت فى الثلاث فئات الأولى كما يلي؛ الفئة الأولى الأقل من 30 سنة، وبلغت نسبتها (11.9%)، الفئة الثانية من 30-39 سنة، وبلغت نسبتها (71.3%)، والفئة الثالثة من 40-49 سنة، وبلغت نسبتها (10.9%)، كما بلغت نسبة الحاصلين على البكالوريوس فقط (49.5%) من العينة، وبلغت نسبة الحاصلين على الماجستير (32.7%) من العينة، بينما بلغت نسبة الحاصلين على درجة الدكتوراه (17.8%). كذلك يتضح من الجدول أن أغلبية المشاركين فى الاستبيان كانوا من الذكور بنسبة (94.1%) والباقى من الإناث. وبالنظر إلى مستوى الخبرة لدى أفراد العينة يتضح أنها تركزت في ثلاث فئات وهي؛ الفئة الأولى من المحاسبين الذين لديهم سنوات خبرة أقل من 5 سنوات، وبلغت نسبتها (11.9%)، الفئة الثانية من المحاسبين الذين لديهم سنوات خبرة من 5-10 سنوات، وبلغت نسبتها (15.8%)، الفئة الثالثة من المحاسبين الذين لديهم سنوات خبرة من 11-15 سنة، وبلغت نسبتها

(56.4%)، الفئة الأخيرة من المحاسبين الذين لديهم سنوات خبرة أكثر من 20 سنة، وبلغت نسبتها (10.9%). نظراً لتباين خصائص العينة من حيث العمر، والمؤهل العلمي، والنوع، وسنوات الخبرة، سيقوم الباحثان بإدراج تلك الخصائص كمتغيرات رقابية عند قياس أثر السمات الشخصية المظلمة للمحاسبين على اتجاهاتهم نحو الإفصاح عن مخاطر الأمن السيبرانى.

5-5 قياس ثبات وصدق محتوى عبارات قائمة الاستبيان

تم إجراء اختبار كرونباخ ألفا Cronbach`s Alpha، لقياس مدى ثبات إجابات المستقصى منهم على الأسئلة المقدمة لهم في ضوء الحالة المرفقة بالدراسة. يوضح الجدول رقم (4) التالي، نتيجة إختبار الفاكرونباخ (معامل الثبات)، ومعامل الصدق للمتغيرات التابعة والمستقلة في الدراسة، حيث تم حساب معامل الصدق عن طريق إيجاد الجذر التربيعي لمعامل الثبات الفا. يُشير معامل الثبات إلى مدى استقرار وثبات النتائج إذا أعُيد تطبيق نفس الحالة على نفس العينة، حيث أن زيادة معامل الثبات تعني زيادة إحتمالية التوصل لنفس قيم المتغيرات البحثية إذا أُعيد توزيع الإستبيان على نفس العينة.

جدول 4: معامل كرونباخ ألفا لعينة الدراسة (Reliability Statistics)

Sample	اختبار الفاكرونباخ	معامل الصدق
المتغيرات التابعة (الإفصاح عن مخاطر الأمن السيبراني)	0.936	0.967
المتغيرات المستقلة (الثالوث المظلم)	0.789	0.888
إجمالي المتغيرات	0.898	0.946

يتضح من الجدول رقم (4) السابق أن معامل كرونباخ ألفا لجميع متغيرات الدراسة بلغت (0.898) بمعامل صدق (0.946)، كما بلغ معامل كرونباخ ألفا للمتغيرات التابعة للدراسة (0.936) بمعامل صدق (0.967)، كما بلغ معامل كرونباخ ألفا للمتغيرات المستقلة للدراسة (0.789) بمعامل صدق (0.888)، وحيث أن المعامل المقبول لقيمة كرونباخ ألفا أكبر من 70% (Sekaran and Bougie 2016)، لذا فإن ذلك يُشير إلى إمكانية تعميم نتائج الدراسة.

5-6 الإحصاء الوصفى لعينة الدراسة

جدول 5: الإحصاء الوصفى لمتغيرات الدراسة

N	Min	Max	Std. Deviation	Median	Mean	المتغيرات
101	1.33	5.00	1.20630	4.3333	3.6865	قبول الإفصاح DISC_ACCEPT (المجموعة الأولى Q1-Q3)
101	1.00	5.00	1.05685	4.0000	3.8350	نغمة الإفصاح DISC_TONE (المجموعة الأولى Q4-Q6)
101	1.00	5.00	1.13253	3.3333	3.4686	التلاعب بالإفصاحDISC_MANIP (المجموعة الأولى Q7-Q9)
101	1.00	4.44	0.82107	3.0000	3.0319	الميكافيللية MACH (المجموعة الثانية Q1-Q9)
101	1.00	3.89	0.64946	3.2222	3.1034	النرجسية NAR (المجموعة الثانية Q10- Q18)
101	1.00	3.26	0.55068	2.2556	2.3007	السيكوباتية PSYC (المجموعة الثانية Q19- Q27)

في ضوء نتائج الجدول رقم (5) السابق يُلاحظ أن متوسط متغير قبول الإفصاح (DISC_ACCEPT) بلغ (3.6865)، بإنحراف معياري (1.20630)، بما يعني تزايد درجة قبول المحاسبين للإفصاح عن مخاطر الأمن السيبراني، فضلاً عن إنخفاض درجة تباين قبول الإفصاح لدى أفراد العينة، كما يُلاحظ أن متوسط متغير نغمة الإفصاح (DISC_TONE) بلغ (3.8350)، بإنحراف معياري (1.05685)، بما يعني وجود توجه كبير للإعتماد على النغمة الإيجابية للإفصاح عن مخاطر الأمن السيبراني من أفراد العينة، فضلاً عن إنخفاض درجة تباين نغمة الإفصاح لدى أفراد العينة. أخيراً يُلاحظ أن متوسط متغير التلاعب في الإفصاح (DISC_MANIP) بلغ (3.4686)، بإنحراف معياري (1.13253)، بما يعني وجود توجه كبير للتلاعب عند الإفصاح عن مخاطر الأمن السيبراني، فضلاً عن إنخفاض درجة تباين متغير التلاعب في الإفصاح لدى أفراد العينة.

وعلى مستوى المتغيرات المستقلة، يُلاحظ أن متوسط الميكافيللية (MACH) بلغ (3.0319)، بإنحراف معياري (0.82107)، بما يُشير إلى وجود الميكافيللية بدرجة متوسطة لدى أفراد العينة، فضلاً عن إنخفاض درجة تباين مستوى الميكافيللية لدى أفراد العينة. يُلاحظ أيضاً إرتفاع مستوى

الميكافيللية لدى بعض الأفراد في العينة، فقد حاز بعض الأفراد على (4.44) في مؤشر الميكافيللية على مقياس ليكرت الخماسي. بلغ متوسط النرجسية (NAR) (3.1034)، بإنحراف معياري (0.64946)، بما يُشير إلى وجود النرجسية بدرجة متوسطة لدى أفراد العينة، فضلاً عن إنخفاض درجة تباين مستوى النرجسية لدى أفراد العينة. كما يُلاحظ إرتفاع درجة النرجسية لدى بعض الأفراد في العينة، حيث حاز بعض الأفراد على (3.89) في مؤشر النرجسية على مقياس ليكرت الخماسي. أخيراً يُلاحظ أن متوسط السيكوباتية (PSYC) بلغ (2.3007)، بإنحراف معياري (0.55068)، بما يُشير إلى إنخفاض مستوى السيكوباتية لدى أفراد العينة، فضلاً عن إنخفاض درجة تباين مستوى السيكوباتية لدى أفراد العينة، كذلك يُلاحظ إنخفاض مؤشر السيكوباتية لدى غالبية الأفراد في العينة، حيث بلغت أعلى قيمة (3.26) على مقياس ليكرت الخماسي.

5-7 إختبار One Sample t-test

قام الباحثان بإجراء إختبار One Sample t-test، وذلك للتعرف على الإتجاه العام للمحاسبين فيما يتعلق بقبول الإفصاح عن مخاطر الإفصاح الأمن السيبراني، وكذلك نغمة الإفصاح، والتلاعب فى الإفصاح. أيضاً يُساهم هذا الإختبار فى التعرف على نتائج قياس متغيرات الثالوث المظلم لدى المحاسبين، والإتجاه العام لهذه المتغيرات في عينة الدراسة. يوضح الجدول رقم (6) التالى نتائج إختبار One Sample t-test للمتغيرات الأساسية للدراسة، وذلك على النحو التالى:

جدول 6: اختبار One-Sample Test

المتغيرات	المتوسط	الإنحراف المعيارى	قيمة الفروق عن القيم المحايدة	قيمة t
قبول الإفصاح DISC_ACCEPT (المجموعة الأولى Q1-Q3)	3.6865	1.20630	0.68647	5.719***
نغمة الإفصاح DISC_TONE (المجموعة الأولى Q4-Q6)	3.8350	1.05685	0.83498	7.940***
التلاعب بالإفصاحDISC_MANIP (المجموعة الأولى Q7-Q9)	3.4686	1.13253	0.46865	4.159***
الميكافيللية MACH (المجموعة الثانية Q1-Q9)	3.0319	0.82107	0.03190	0.390
النرجسية NAR (المجموعة الثانية Q10-Q18)	3.1034	0.64946	0.10341	1.600
السيكوباتية PSYC (المجموعة الثانية Q19-Q27)	2.3007	0.55068	- 0.69934	-7.688***

حيث إن * تعني أن العلاقة دالة عند مستوى معنوية أقل من 10%، ** تعني أن العلاقة دالة عند مستوى معنوية أقل من 5%، *** تعني أن العلاقة دالة عند مستوى معنوية أقل من 1%.

يوضح الجدول رقم (6) السابق مدى إختلاف متوسط القيم لمتغيرات الدراسة عن القيمة المحايدة على مقياس ليكرت الخماسي وهي نقطة الوسط "3" (Daugherty et al. 2012). تُشير النتائج إلى زيادة مستوى قبول الإفصاح عن مخاطر الأمن السيبراني من قبل أفراد العينة (DISC_ACCEPT)، وتوجههم نحو النغمة الإيجابية للإفصاح (DISC_TONE)، والتوجه نحو التلاعب عند الإفصاح عن مخاطر الأمن السيبراني (DISC_MANIP)، حيث يزداد متوسط تلك المتغيرات بشكل معنوي عن القيمة المحايدة "3"، وذلك عند مستوى معنوية أقل من (1%). كما يُلاحظ زيادة مستوى الميكافيللية (MACH) والنرجسية (NAR) في عينة الدراسة عن القيمة المحايدة"3"، إلا أن تلك الزيادة ليست معنوية. بينما تُشير النتائج إلى إنخفاض مستوى السيكوباتية في عينة الدراسة عن القيمة المحايدة "3"، وذلك عند مستوى معنوية أقل من (1%)، الأمر الذي يعني إنخفاض هذا المتغير لدى أفراد العينة، لذا يتوقع الباحثان عدم وجود تأثير معنوي لمتغير السيكوباتية (PSYC) على الإفصاح عن مخاطر الأمن السيبراني. حيث تؤكد نتائج بعض الدراسات السابقة على أن الآثار السلبية للثالوث المظلم تظهر فقط في المستويات العليا (Amernic and Craig 2010; Murphy 2012; Rijsenbilt and Commandeur 2013).

5-8 مصفوفة ارتباط بيرسون لمتغيرات العينة

قام الباحثان بتحليل الارتباط بين المتغيرات البحثية للدراسة، ويوضح الجدول رقم (7) التالى مصفوفة ارتباط بيرسون.

جدول 7: مصفوفة الارتباط بين المتغيرات البحثية

	Disc_Accept	Disc_Tone	Disc_Manip	MACH	NAR	PSYC	Gender	Age	Qualifications	Expert
Disc_Accept	1									
Disc_Tone	0.825***	1								
Disc_Manip	0.830***	0.849***	1							
MACH	0.613***	0.635***	0.705***	1						
NAR	0.600***	0.734***	0.603***	0.768***	1					
PSYC	0.308***	0.393***	0.293***	0.412***	0.506***	1				
Gender	-0.283***	0.039	-0.253**	-0.249**	0.003	-.123	1			
Age	-0.019-	-0.128-	-0.028-	-0.130-	-0.291***	-0.204**	-.041	1		
Qualifications	-0.454***	-0.551***	-0.325***	-0.252**	-0.302***	-0.374***	-0.227**	0.087	1	
Expert	0.353***	0.426***	0.313***	0.223**	0.219**	0.291***	0.031	0.496***	-0.263***	1

حيث إن * تعني أن العلاقة دالة عند مستوى معنوية أقل من 10%، ** تعني أن العلاقة دالة عند مستوى معنوية أقل من 5%، *** تعني أن العلاقة دالة عند مستوى معنوية أقل من 1%.

فى ضوء الجدول رقم (7) السابق يُلاحظ وجود علاقة ارتباط إيجابية بين كل من الميكافيللية (MACH)، والنرجسية (NAR)، والسيكوباتية (PSYC)، وبين مدى قبول المحاسبين للإفصاح عن مخاطر الأمن السيبرانى (DISC_ACCEPT) وذلك عند مستوى معنوية أقل من (1%). بما يُشير إلى زيادة مدى قبول أفراد العينة للإفصاح عن مخاطر الأمن السيبراني مع إرتفاع مستوى الميكافيللية أو النرجسية أو السيكوباتية لديهم. توجد علاقة ارتباط إيجابية بين كل من الميكافيللية (MACH)، والنرجسية (NAR)، والسيكوباتية (PSYC)، وبين النغمة الإيجابية للإفصاح عن مخاطر الأمن السيبرانى (DISC_TONE) وذلك أيضاً عند مستوى معنوية أقل من (1%). بما يُشير إلى زيادة توجه أفراد العينة لإستخدام النغمة الإيجابية للإفصاح عن مخاطر الأمن السيبراني مع إرتفاع مستوى الميكافيللية أو النرجسية أو السيكوباتية لديهم. أخيراً يُلاحظ وجود علاقة ارتباط إيجابية بين كلٍ من الميكافيللية (MACH)، والنرجسية (NAR)، والسيكوباتية (PSYC)، وبين إحتمالية التلاعب عند الإفصاح عن مخاطر الأمن السيبرانى وذلك عند مستوى معنوية أقل من (1%)، بما يُشير إلى زيادة توجه أفراد العينة للتلاعب عند الإفصاح عن هذه المخاطر مع إرتفاع مستوى الميكافيللية أو النرجسية أو السيكوباتية لديهم.

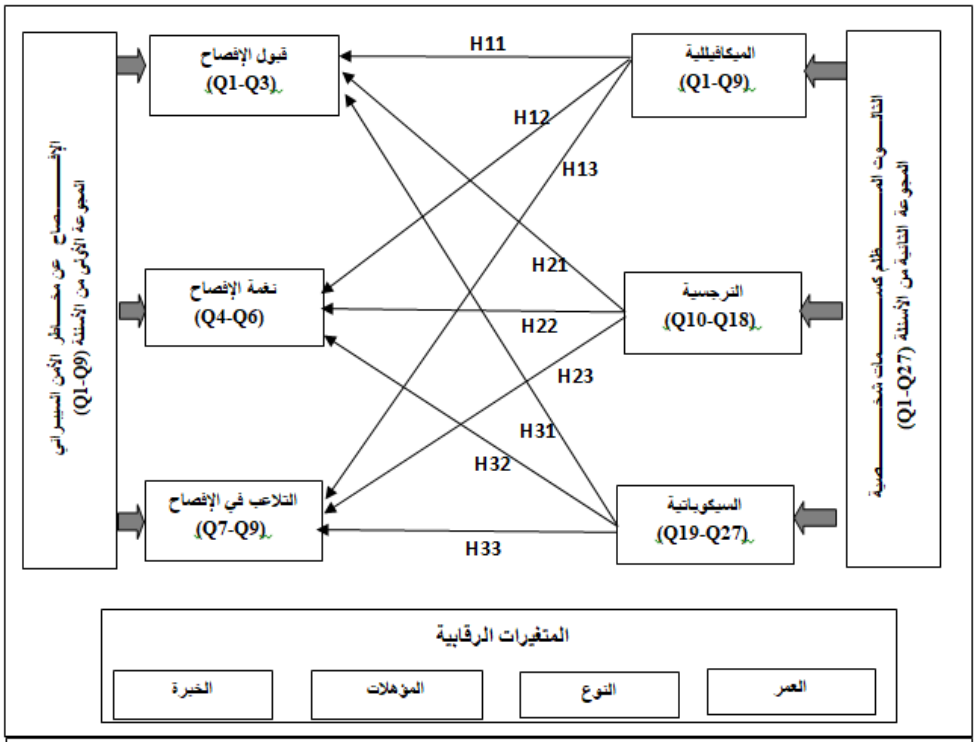
أظهرت مصفوفة الارتباط وجود علاقة ارتباط إيجابية بين الميكافيللية (MACH)، وبين كل من النرجسية (NAR)، والسيكوباتية (PSYC)، تلك النتائج تتوافق مع نتائج بعض الدراسات السابقة في مجال الثالوث المظلم والتي تؤكد على وجود سمات مشتركة بين الميكافيللين والنرجسيين والسيكوباتيين (Furnham et al. 2013; Maasberg et al. 2020; Mutschmann et al. 2021). كما أظهرت مصفوفة الارتباط وجود علاقة ارتباط إيجابية بين كل من الميكافيللية (MACH)، والنرجسية (NAR)، والسيكوباتية (PSYC)، وبين سنوات الخبرة لدى أفراد العينة وذلك عند مستوى معنوية أقل من (5%) لكل من الميكافيللية والنرجسية، و مستوى معنوية أقل من (1%) للسيكوباتية. فى حين لم نجد أية علاقة ارتباط معنوية بين النوع وبين كلٍ من النرجسية (NAR) والسيكوباتية (PSYC)، بينما كانت هناك علاقة ارتباط سلبية عند مستوى معنوية أقل من (5%) بين النوع والميكافيللية. الأمر الذي يعني إنخفاض مستوى الميكافيللية لدى الإناث مقارنة بالذكور.

أظهرت مصفوفة الارتباط أيضاً وجود علاقة ارتباط سلبية بين كل من الميكافيللية (MACH)، والنرجسية (NAR)، والسيكوباتية (PSYC)، وبين المؤهل العلمي وذلك عند مستوى أقل من (1%)، بما يعني انخفاض مستوى الثالوث المظلم لدى الأفراد الحاصلين على مؤهل علمي أعلى من البكالوريوس، أخيراً يُلاحظ وجود علاقة سلبية غير معنوية بين العمر ومستوى الميكافيللية

(MACH)، بينما توجد علاقة سلبية معنوية بين العمر وبين كلٍ من النرجسية (NAR)، والسيكوباتية (PSYC)، وذلك عند مستوى معنوية أقل من (1%)، (5%) على التوالي.

5-9 نموذج الدراسة

يوضح الشكل التالى رقم (1) نموذج الدراسة المستخدم، من حيث المتغيرات المستقلة، والمتغيرات التابعة، والمتغيرات الرقابية، وذلك على النحو التالى:



شكل 1: نموذج الدراسة

المصدر: إعداد الباحثان

5-10 نتائج اختبار فروض الدراسة

5-10-1 اختبار الفرض الرئيس الأول (H1)

يستهدف الفرض الرئيس الأول اختبار تأثير الميكافيللية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على اتجاهاتهم نحو الإفصاح عن مخاطر الأمن السيبراني. وينبثق عن هذا الفرض مجموعة من الفروض الفرعية التالية:

الفرض الفرعى الأول (H11): يوجد تأثير إيجابي معنوي للميكافيلية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على مدى قبولهم للإفصاح عن مخاطر الأمن السيبراني. لاختبار هذا الفرض، سيتم تشغيل نموذج الإنحدار التالي بطريقة المربعات الصغرى:

$$DISC\_ACCEPT = B_0 + B_1\ MACH + B_2\ Gender + B_3\ Age + B_4\ Qualification + B_5\ Expert + \varepsilon \quad (1)$$

يوضح الجدول رقم (8) نتائج تحليل نموذج الانحدار رقم (1).

جدول 8: نتائج تحليل نموذج الانحدار رقم (1)

Variables	β	Std.Error	t	Sig	Collinearity statistics	
					Tolerance	VIF
Constant	3.816	0.771	4.947	0.000	-	-
MACH	0.594	0.115	5.168	0.000	0.759	1.318
Gender	-1.380	0.378	-3.654	0.000	0.840	1.190
Age	-0.080	0.150	-0.536	0.593	0.655	1.526
Qualification	- 0.567	0.122	-4.651	0.000	0.786	1.272
Expert	0.228	0.100	2.280	0.025	0.607	1.647
R^2= 0.559 Adj R^2 =0. 535						
F= 24.036 Sig= 0 .000						

ويلاحظ الباحثان تعليقاً على الجدول رقم (8) السابق ما يلي:

بلغت قيمة Adjusted R^2 (0.535)، وذلك يعني أن النموذج وما إشتمل عليه من متغيرات يمكنه تفسير 53.5% من التغير الكلى فى قيمة المتغير التابع (قبول الإفصاح DISC_ACCEPT)، وباقى النسبة قد ترجع إلى عدم إدراج بعض المتغيرات المستقلة الأخرى ذات التأثير، أو إلى الخطأ العشوائى. أوضحت نتائج إختبار Variance Inflation Factor(VIF) لإختبار مشكلة الإزدواج الخطي في نموذج الإنحدار، أن قيمة (VIF) أقل من (10)، بما يُشير إلى أن نموذج الإنحدار لا يعانى من مشكلة الإزدواج الخطى (Sekaran and Bougie 2016).

يوضح الجدول رقم (8) السابق وجود تأثير إيجابي للميكافيللية (MACH) كأحد أبعاد الثالوث المظلم للشخصية على مدى قبول المحاسبين للإفصاح عن مخاطر الأمن السيبرانى، وذلك عند مستوى معنوية أقل من (1%)، الأمر الذى يعنى زيادة مستوى قبول الميكافيلليين للإفصاح عن مخاطر الأمن السيبرانى، فى محاولة لاستغلال هذا النوع من الإفصاح لتحقيق الترويج الذاتي Self–promotion، إنهم قادرون على إستغلال كل شيئ لتحقيق رؤيتهم الاستراتيجية (Bailey

(Maasberg et al.2020;2015. لذا نتوقع أن يحمل هذا القبول فى طياته بعض الإستراتيجيات الأخرى التى قد تكون أكثر ضرراً من الرفض، كالإعتماد على النغمة الإيجابية والتلاعب عند الإفصاح عن مخاطر الأمن السيبراني، وهو ما سيتضح عند اختبار الفرضين الفرعيين الثانى (H12) والثالث (H13). **وبناءً على ذلك سيتم قبول الفرض الفرعي (H11).**

وفيما يخص المتغيرات الرقابية، يؤثر كلٍ من (النوع Gender، المؤهل العلمىQualifications) تأثيراً سلبياً على مدى قبول المحاسبون للإفصاح عن مخاطر الأمن السيبرانى، وذلك عند مستوى معنوية أقل من (1%). بينما يوجد تأثير إيجابي لسنوات الخبرة (Expert) على مدى قبول المحاسبون للإفصاح عن مخاطر الأمن السيبرانى وذلك عند مستوى معنوية أقل من (5%). فى حين يوجد تأثير إيجابي غير معنوى للعمر (Age) على مدى قبول المحاسبون للإفصاح عن مخاطر الأمن السيبراني.

الفرض الفرعى الثانى (H12): يوجد تأثير إيجابي معنوي للميكافيللية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على نغمة الإفصاح الإيجابية عن مخاطر الأمن السيبراني. لاختبار هذا الفرض، سيتم تشغيل نموذج الإنحدار التالي بطريقة المربعات الصغرى:

$$DISC\_TONE = B_0 + B_1\ MACH + B_2\ Gender + B_3\ Age + B_4\ Qualification + B_5\ Expert + \varepsilon \quad (2)$$

يوضح الجدول رقم (9) نتائج تحليل نموذج الانحدار رقم (2).

جدول 9: نتائج تحليل نموذج الانحدار رقم (2)

Variables	β	Std.Error	t	Sig	Collinearity statistics	
					Tolerance	VIF
Constant	2.097	0.607	3.455	0.001	-	-
MACH	0.607	0.090	6.711	0.000	0.759	1.318
Gender	0.302	0.297	1.018	0.311	0.840	1.190
Age	-0.321	0.118	-2.720	0.008	0.655	1.526
Qualification	-0.429	0.096	-4.475	0.000	0.786	1.272
Expert	0.340	0.079	4.321	0.000	0.607	1.647
R^2= 0.644 Adj R^2 =0.625						
F= 34.335 Sig= 0 .000						

ويلاحظ الباحثان تعليقاً على الجدول رقم (9) السابق ما يلي:

بلغت قيمة Adjusted R^2 (0.625)، وذلك يعني أن النموذج وما إشتمل عليه من متغيرات يمكنه تفسير 62.5% من التغير الكلى فى قيمة المتغير التابع (نغمة الإفصاح DISC_TONE)، وباقى النسبة قد ترجع إلى عدم إدراج بعض المتغيرات المستقلة الأخرى ذات التأثير، أو إلى الخطأ العشوائى. أوضحت نتائج إختبار (VIF) لإختبار مشكلة الإزدواج الخطي في نموذج الإنحدار، أن قيمة (VIF) أقل من (10)، بما يُشير إلى أن نموذج الإنحدار لا يعانى من مشكلة الإزدواج الخطى (Sekaran and Bougie 2016).

كذلك يوضح الجدول رقم (9) السابق وجود تأثير إيجابي للميكافيللية (MACH) كأحد أبعاد الثالوث المظلم للشخصية على نغمة الإفصاح الإيجابية، وذلك عند مستوى معنوية أقل من (1%). بما يُشير إلى توجه الميكافيلليون نحو تبني النغمة الإيجابية، لإهتمامهم المتزايد بالسمعة، وكذلك لطمأنة المستثمرين، استكمالاً لاستراتيجيتهم التى تقوم على الخداع والغش للآخرين. **وبناءً على ذلك سيتم قبول الفرض الفرعي (H12).**

وفيما يخص المتغيرات الرقابية، يؤثر كلٍ من (العمر Age، المؤهل العلمى Qualifications) تأثيراً سلبياً على نغمة الإفصاح الإيجابية، وذلك عند مستوى معنوية أقل من (1%). بينما يوجد تأثير إيجابي لسنوات الخبرة (Expert) على نغمة الإفصاح الإيجابية، وذلك عند مستوى معنوية أقل من (1%). فى حين يوجد تأثير إيجابي غير معنوى للنوع (Gender) على نغمة الإفصاح الإيجابية عن مخاطر الأمن السيبراني.

الفرض الفرعى الثالث (H13) يوجد تأثير إيجابي معنوي للميكافيللية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على إحتمالية التلاعب بالمعلومات المرتبطة بمخاطر الأمن السيبراني. لاختبار هذا الفرض، سيتم تشغيل نموذج الإنحدار التالي بطريقة المربعات الصغرى:

$$DISC\_MANIP = B_0 + B_1\ MACH + B_2\ Gender + B_3\ Age + B_4\ Qualification + B_5\ Expert + \varepsilon \quad (3)$$

يوضح الجدول رقم (10) نتائج تحليل نموذج الانحدار رقم (3).

جدول 10: نتائج تحليل نموذج الانحدار رقم (3)

Variables	β	Std.Error	t	Sig	Collinearity statistics	
					Tolerance	VIF
Constant	1.789	0.727	2.462	0.016	-	-
MACH	0.812	0.108	7.497	0.000	0.759	1.318
Gender	-0.717	0.356	-2.016	0.047	0.840	1.190
Age	-0.029	0.141	-0.208	0.836	0.655	1.526
Qualification	-0.252	0.115	-2.197	0.030	0.786	1.272
Expert	0.162	0.094	1.718	0.089	0.607	1.647
R^2= 0. .556 Adj R^2 =0. .532						
F= 23.759 Sig= 0 .000						

ويلاحظ الباحثان تعليقاً على الجدول رقم (10) السابق ما يلي:

بلغت قيمة Adjusted R^2 (0.532)، وذلك يعني أن النموذج وما إشتمل عليه من متغيرات يمكنه تفسير 53.2% من التغير الكلى فى قيمة المتغير التابع (التلاعب بالإفصاح DISC_MANIP)، وباقى النسبة قد يرجع إلى عدم إدراج متغيرات مستقلة أخرى ذات تأثير، أو إلى الخطأ العشوائى. أوضحت نتائج إختبار Variance Inflation Factor(VIF) لإختبار مشكلة الإزدواج الخطي في نموذج الإنحدار، أن قيمة (VIF) أقل من (10)، بما يُشير إلى أن نموذج الإنحدار لا يعانى من مشكلة الإزدواج الخطى (Sekaran and Bougie 2016).

كذلك يوضح الجدول رقم (10) السابق وجود تأثير إيجابي للميكافيللية (MACH) كأحد أبعاد الثالوث المظلم للشخصية على إحتمالية التلاعب بالمعلومات المرتبطة بمخاطر الأمن السيبراني، وذلك عند مستوى معنوية أقل من (1%)، الأمر الذى يشير إلى زيادة إحتمالية قيام الميكافيللون بالتلاعب والتحايل من أجل عدم الإفصاح عن المخاطر قدر الإمكان، وتجنب الإفصاح عن محاولات الإختراق السابقة أو المحتملة. **وبناءً على ذلك سيتم قبول الفرض الفرعي (H13).**

وفيما يخص المتغيرات الرقابية، يؤثر كلٍ من (النوعGender، المؤهل العلمىQualifications) تأثيراً سلبياً على إحتمالية التلاعب بالمعلومات المرتبطة بمخاطر الأمن السيبراني وذلك عند مستوى معنوية أقل من (5%). بينما يوجد تأثير إيجابي لسنوات الخبرة (Expert) على إحتمالية التلاعب بالمعلومات المرتبطة بمخاطر الأمن السيبراني وذلك عند مستوى معنوية أقل من (10%). فى حين يوجد تأثير سلبي غير معنوى للعمر (Age) على إحتمالية التلاعب بالمعلومات المرتبطة بمخاطر الأمن السيبرانى.

فى ضوء نتائج اختبار الفروض الفرعية الثلاث السابقة، سيتم **قبول الفرض الرئيس الأول (H1) القائل بوجود تأثير إيجابي معنوي للميكافيللية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على اتجاهاتهم نحو الإفصاح عن مخاطر الأمن السيبراني**".

وتتفق هذه النتيجة مع ما توصل إليه بعض الباحثين (Shafer and Wang 2011; Vladu 2013; Harrison et al. 2018; Utami et al. 2019; Murphy 2012). والذين أكدوا على أن الأفراد الذين حصلوا على درجات عالية في اختبار الميكافيللية يميلون للتلاعب بدرجة أكبر وينخفض لديهم الشعور بالذنب، حيث تُحفز الميكافيللية الأفراد على التصرف بشكل غير أخلاقي، ويفترضون غالباً أن الآخرين سيتخذون نفس القرارات غير الأخلاقية، ولا مانع لديهم من تغيير الحقائق لخداع الآخرين وممارسة الغش والإحتيال المالي بشكل أكبر.

5-10-2 اختبار الفرض الرئيس الثاني (H2)

يستهدف الفرض الرئيس الثاني اختبار تأثير النرجسية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على اتجاهاتهم نحو الإفصاح عن مخاطر الأمن السيبراني. وينبثق عن هذا الفرض مجموعة الفروض الفرعية التالية:

الفرض الفرعى الأول (H21): يوجد تأثير إيجابي معنوي للنرجسية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على مدى قبولهم للإفصاح عن مخاطر الأمن السيبراني. لاختبار هذا الفرض، سيتم تشغيل نموذج الإنحدار التالي بطريقة المربعات الصغرى:

$$DISC\_ACCEPT = B_0 + B_1\ NAR + B_2\ Gender + B_3\ Age + B_4\ Qualification + B_5\ Expert + \varepsilon \quad (4)$$

يوضح الجدول رقم (11) نتائج تحليل نموذج الانحدار رقم (4).

جدول 11: نتائج تحليل نموذج الانحدار رقم (4)

Variables	β	Std.Error	t	Sig	Collinearity statistics	
					Tolerance	VIF
Constant	3.137	0.753	4.164	0.000	-	-
NAR	0.905	0.142	6.391	0.000	0.716	1.396
Gender	-1.870	0.338	-5.539	0.000	0.942	1.062
Age	0.141	0.152	0.928	0.356	0.570	1.755
Qualification	-0.580	0.114	-5.075	0.000	0.802	1.247
Expert	0.140	0.098	1.424	0.158	0.567	1.763
R^2= 0.604 Adj R^2 =0.584						
F= 29.036 Sig= 0 .000						

ويلاحظ الباحثان تعليقاً على الجدول رقم (11) السابق ما يلي:

بلغت قيمة Adjusted R^2 (0.584)، وذلك يعني أن النموذج وما إشتمل عليه من متغيرات يمكنه تفسير 58.4% من التغير الكلى فى قيمة المتغير التابع (قبول الإفصاح DISC_ACCEPT)، وباقى النسبة قد ترجع إلى عدم إدراج بعض المتغيرات المستقلة الأخرى ذات التأثير، أو إلى الخطأ العشوائى. أوضحت نتائج إختبار (VIF) لإختبار مشكلة الإزدواج الخطي في نموذج الإنحدار، أن قيمة (VIF) أقل من (10)، بما يُشير إلى أن نموذج الإنحدار لا يعانى من مشكلة الإزدواج الخطى (Sekaran and Bougie 2016).

يوضح الجدول رقم (11) السابق وجود تأثير إيجابي للنرجسية (NAR) كأحد أبعاد الثالوث المظلم للشخصية على مدى قبول المحاسبين للإفصاح عن مخاطر الأمن السيبرانى، وذلك عند مستوى معنوية أقل من (1%)، الأمر الذى يعني تزايد قبول النرجسيون للإفصاح عن مخاطر الأمن السيبرانى، لقدرتهم على إستغلال هذا النوع من الإفصاح للحصول على الثناء المتكرر والإعجاب، ودعم صورتهم الذاتية الرائعة(Lassoued and Khanchel 2022). وهو ما سيتضح عند اختبار الفرضين الفرعيين الثانى (H22) والثالث (H23). **وبناءً على ذلك سيتم قبول الفرض الفرعي الأول (H21).**

وفيما يخص المتغيرات الرقابية، يؤثر كلٍ من (النوع Gender، المؤهل العلمىQualifications) تأثيراً سلبياً على مدى قبول المحاسبون للإفصاح عن مخاطر الأمن السيبرانى، وذلك عند مستوى معنوية أقل من (1%). فى حين يوجد تأثير إيجابي غير معنوى للعمر (Age) ولسنوات الخبرة (Expert) على مدى قبول المحاسبون للإفصاح عن مخاطر الأمن السيبرانى.

الفرض الفرعى الثانى (H22): يوجد تأثير إيجابي معنوي للنرجسية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على نغمة الإفصاح الإيجابية عن مخاطر الأمن السيبراني. لاختبار هذا الفرض، سيتم تشغيل نموذج الإنحدار التالي بطريقة المربعات الصغرى:

$$DISC\_TONE = B_0 + B_1\ NAR + B_2\ Gender + B_3\ Age + B_4\ Qualification + B_5\ Expert + \varepsilon \quad (5)$$

يوضح الجدول رقم (12) نتائج تحليل نموذج الانحدار رقم (5).

جدول 12: نتائج تحليل نموذج الانحدار رقم (5)

Variables	β	Std.Error	t	Sig	Collinearity statistics	
					Tolerance	VIF
Constant	1.424	0.571	2.492	0.014	-	-
NAR	0.919	0.107	8.560	0.000	0.716	1.396
Gender	-0.200	0.256	-0.780	0.437	0.942	1.062
Age	-0.097	0.116	-0.841	0.403	0.570	1.755
Qualification	-0.443	0.087	-5.115	0.000	0.802	1.247
Expert	0.251	0.074	3.379	0.001	0.567	1.763
R^2= 0.704 Adj R^2 =0.688						
F= 45.089 Sig= 0 .000						

ويلاحظ الباحثان تعليقاً على الجدول رقم (12) السابق ما يلي:

بلغت قيمة Adjusted R^2 (0.688) وذلك يعني أن النموذج وما إشتمل عليه من متغيرات يمكنه تفسير 68.8% من التغير الكلى فى قيمة المتغير التابع (نغمة الإفصاح DISC_TONE)، وباقى النسبة قد ترجع إلى عدم إدراج بعض المتغيرات المستقلة الأخرى ذات التأثير، أو إلى الخطأ العشوائى. أوضحت نتائج إختبار (VIF) لإختبار مشكلة الإزدواج الخطي في نموذج الإنحدار، أن قيمة (VIF) أقل من (10)، بما يُشير إلى أن نموذج الإنحدار لا يعانى من مشكلة الإزدواج الخطى (Sekaran and Bougie 2016).

يوضح الجدول رقم (12) السابق وجود تأثير إيجابي للنرجسية (NAR) كأحد أبعاد الثالوث المظلم للشخصية على نغمة الإفصاح الإيجابية عن مخاطر الأمن السيبراني، وذلك عند مستوى معنوية أقل من (1%)، الأمر الذي يعني توجه النرجسيون للإفصاح عن الجوانب الإيجابية التي تُطمئن المستثمرين، وتعزز لديهم الشعور بالعظمة، وتدعم سمعتهم. تتفق تلك النتائج مع بعض الدراسات السابقة في مجال النرجسية الإدارية والإفصاح المحاسبي (Marquez-Illescas et al. 2019; Lassoued and Khanchel 2022). **وبناءً على ذلك سيتم قبول الفرض الفرعي (H22).**

وفيما يخص المتغيرات الرقابية، يُلاحظ وجود تأثير سلبي للمؤهل العلمي (Qualifications) على نغمة الإفصاح الإيجابية عن مخاطر الأمن السيبراني، وذلك عند مستوى معنوية أقل من (1%). بينما يوجد تأثير إيجابي لسنوات الخبرة (Expert) على نغمة الإفصاح الإيجابية، وذلك

عند مستوى معنوية أقل من (1%). فى حين يوجد تأثير سلبي غير معنوى لكلٍ من (العمر Age، النوع Gender) على نغمة الإفصاح الإيجابية عن مخاطر الأمن السيبراني.

الفرض الفرعى الثالث (H23): يوجد تأثير إيجابي معنوي للنرجسية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على إحتمالية التلاعب بالمعلومات المرتبطة بمخاطر الأمن السيبراني. لاختبار هذا الفرض، سيتم تشغيل نموذج الإنحدار التالي بطريقة المربعات الصغرى:

$$DISC\_MANIP = B_0 + B_1\ NAR + B_2\ Gender + B_3\ Age + B_4\ Qualification + B_5\ Expert + \varepsilon \quad (6)$$

يوضح الجدول رقم (13) نتائج تحليل نموذج الانحدار رقم (6).

جدول 13: نتائج تحليل نموذج الانحدار رقم (6)

Variables	β	Std.Error	t	Sig	Collinearity statistics	
					Tolerance	VIF
Constant	1.968	0.793	2.481	0.015	-	-
NAR	0.943	0.149	6.327	0.000	0.716	1.396
Gender	-1.441	0.355	-4.053	0.000	0.942	1.062
Age	0.136	0.160	0.850	0.397	0.570	1.755
Qualification	-0.311	0.120	-2.584	0.011	0.802	1.247
Expert	0.117	0.103	1.130	0.261	0.567	1.763
R^2= 0. .502 Adj R^2 =0. .476						
F= 19.186 Sig= 0 .000						

ويلاحظ الباحثان تعليقاً على الجدول رقم (13) السابق ما يلي:

بلغت قيمة Adjusted R^2 (0.476) وذلك يعني أن النموذج وما إشتمل عليه من متغيرات يمكنه تفسير 47.6% من التغير الكلى فى قيمة المتغير التابع (التلاعب بالإفصاح DISC_MANIP)، وباقى النسبة قد ترجع إلى عدم إدراج بعض المتغيرات المستقلة الأخرى ذات التأثير، أو إلى الخطأ العشوائى. أوضحت نتائج إختبار (VIF) لإختبار مشكلة الإزدواج الخطي في نموذج الإنحدار، أن قيمة (VIF) أقل من (10)، بما يُشير إلى أن نموذج الإنحدار لا يعانى من مشكلة الإزدواج الخطى (Sekaran and Bougie 2016).

يوضح الجدول رقم (13) السابق وجود تأثير إيجابي للنرجسية (NAR) كأحد أبعاد الثالوث المظلم للشخصية على إحتمالية التلاعب بالمعلومات المرتبطة بمخاطر الأمن السيبراني، وذلك عند مستوى معنوية أقل من (1%)، الأمر الذى يشير إلى تزايد إحتمالية التلاعب بالإفصاح عن

معلومات مخاطر الأمن السيبراني مع تزايد النرجسية لدى المحاسبين. تلك النتائج تتشابه إلى حد كبير مع نتائج بعض الدراسات السابقة والتي أكدت على تورط النرجسيون في ممارسات تضليل القوائم المالية، والغش المحاسبي (Ramamoorti 2008; Rijsenbilt and Commandeur 2013; Ham et al. 2017; Capalbo et al. 2018; Buchholz et al. 2019; Mutschmann et al. 2021). **وبناءً على ذلك سيتم قبول الفرض الفرعي (H23).**

وفيما يخص المتغيرات الرقابية، يُلاحظ وجود تأثير سلبي للمؤهل العلمى (Qualifications) على إحتمالية التلاعب بالمعلومات المرتبطة بمخاطر الأمن السيبراني، وذلك عند مستوى معنوية أقل من (1%). بينما يوجد تأثير سلبي للنوع (Gender) على إحتمالية التلاعب بالمعلومات المرتبطة بمخاطر الأمن السيبرانى، وذلك عند مستوى معنوية أقل من (1%). فى حين يوجد تأثير إيجابي غير معنوى لكلٍ من (سنوات الخبرة Expert، والعمر Age) على إحتمالية التلاعب بالمعلومات المرتبطة بمخاطر الأمن السيبراني.

فى ضوء نتائج اختبار الفروض الفرعية الثلاث السابقة، **سيتم قبول الفرض الرئيس الثاني (H2) القائل بوجود تأثير إيجابي معنوي للنرجسية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على اتجاهاتهم نحو الإفصاح عن مخاطر الأمن السيبراني.**

وتتفق هذه النتيجة مع ما توصلت إليه نتائج الدراسات السابقة (Chatterjee and Pollock 2016; Young et al. 2014; Ham et al. 2017; Rijsenbilt and Commandeur 2013; Capalbo et al. 2018; Buchholz et al. 2019; Lassoued and Khanchel (2022، والتى أكدت على أن السمات الشخصية للنرجسيين قائمة على الإستعراض وجذب الإنتباه Exhibitionism، ومحاولة استغلال الآخرين، والتورط في ممارسات الغش المحاسبي، فضلاً عن سماتهم الشخصية التي تُسهل السلوك الاحتيالي من خلال إستغلال الفرص المتاحة، والتبرير العقلي.

5-10-3 اختبار الفرض الرئيس الثالث (H3)

يستهدف الفرض الرئيس الثالث اختبار تأثير السيكوباتية كسمة شخصية للمحاسبين فى البنوك العاملة فى مصر على اتجاهاتهم نحو الإفصاح عن مخاطر الأمن السيبراني، وينبثق عن هذا الفرض مجموعة الفروض الفرعية التالية:

الفرض الفرعى الأول (H31): يوجد تأثير إيجابي معنوي للسيكوباتية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على مدى قبولهم للإفصاح عن مخاطر الأمن السيبراني. لاختبار هذا الفرض، سيتم تشغيل نموذج الإنحدار التالي بطريقة المربعات الصغرى:

$$DISC\_ACCEPT = B_0 + B_1\ PSYC + B_2\ Gender + B_3\ Age + B_4\ Qualification + B_5\ Expert + \varepsilon\ (7)$$

يوضح الجدول رقم (14) نتائج تحليل نموذج الانحدار رقم (7).

جدول 14: نتائج تحليل نموذج الانحدار رقم (7)

Variables	β	Std.Error	t	Sig	Collinearity statistics	
					Tolerance	VIF
Constant	6.963	0.964	7.223	0.000	-	-
PSYC	- 0.116	0.207	-0.560	0.577	0.666	1.502
Gender	-2.093	0.415	-5.047	0.000	0.889	1.124
Age	-0.320	0.177	-1.809	0.074	0.602	1.660
Qualification	-0.730	0.141	-5.191	0.000	0.755	1.325
Expert	0.399	0.118	3.391	0.001	0.560	1.785
R^2= 0.436 Adj R^2 =0. .407						
F= 14.703 Sig= 0 .000						

ويلاحظ الباحثان تعليقاً على الجدول رقم (14) السابق ما يلي:

بلغت قيمة Adjusted R^2 (0.407)، وذلك يعني أن النموذج وما إشتمل عليه من متغيرات يمكنه تفسير 40.7% من التغير الكلى فى قيمة المتغير التابع (قبول الإفصاح DISC_ACCEPT)، وباقى النسبة قد ترجع إلى عدم إدراج بعض المتغيرات المستقلة الأخرى ذات التأثير، أو إلى الخطأ العشوائى.أوضحت نتائج إختبار (VIF) لإختبار مشكلة الإزدواج الخطي في نموذج الإنحدار، أن قيمة (VIF) أقل من (10)، بما يُشير إلى أن نموذج الإنحدار لا يعانى من مشكلة الإزدواج الخطى (Sekaran and Bougie 2016).

يوضح الجدول رقم (14) السابق وجود تأثير سلبي غير معنوى للسيكوباتية (PSYC) كأحد أبعاد الثالوث المظلم للشخصية على مدى قبول المحاسبين للإفصاح عن مخاطر الأمن السيبرانى. تلك النتيجة تتعارض مع نتائج بعض الدراسات السابقة التي أكدت على ممارسة السيكوباتيون للسحر السطحي Superficial Charm؛ والذي يعني توجه الفرد السيكوباتي لقول الأشياء التي يستقبلها الآخرون جيداً، وليس ما يعتقده هو (Hare 1991; Fehr et al. 1992). يرى الباحثان

أن تلك النتيجة ترجع لإنخفاض المستوى العام للسيكوباتية الشخصية لدى أفراد العينة، لذلك لم تظهر أية آثار سلبية على مدى قبول المحاسبين للإفصاح عن مخاطر الأمن السيبراني، وهو ما سبق الإشارة إليه في تحليل One Sample t–test. **بناءً على ذلك سوف يتم رفض الفرض الفرعي (H31).**

بخصوص المتغيرات الرقابية، يُلاحظ وجود تأثير سلبي لكلٍ من (النوع Gender، المؤهل العلمىQualifications) على مدى قبول الإفصاح عن مخاطر الأمن السيبرانى، وذلك عند مستوى معنوية أقل من (1%). بينما يوجد تأثير إيجابي لسنوات الخبرة (Expert) على مدى قبول الإفصاح عن مخاطر الأمن السيبرانى، وذلك عند مستوى معنوية أقل (1%). فى حين يوجد تأثير سلبي غير معنوى للعمر (Age) على مدى قبول المحاسبين للإفصاح عن مخاطر الأمن السيبراني.

الفرض الفرعى الثاني (H32): يوجد تأثير إيجابي معنوي للسيكوباتية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على نغمة الإفصاح الإيجابية عن مخاطر الأمن السيبراني. لاختبار هذا الفرض، سيتم تشغيل نموذج الإنحدار التالي بطريقة المربعات الصغرى:

$$DISC\_TONE = B_0 + B_1\,PSYC + B_2\,Gender + B_3\,Age + B_4\,Qualification + B_5\,Expert + \varepsilon \quad (8)$$

يوضح الجدول رقم (15) نتائج تحليل نموذج الانحدار رقم (8).

جدول 15: نتائج تحليل نموذج الانحدار رقم (8)

Variables	β	Std.Error	t	Sig	Collinearity statistics	
					Tolerance	VIF
Constant	4.712	0.815	5.784	0.000	-	-
PSYC	0.053	0.175	0.301	0.764	0.666	1.502
Gender	-0.342	0.351	-0.975	0.332	0.889	1.124
Age	-0.511	0.150	-3.415	0.001	0.602	1.660
Qualification	-0.562	0.119	-4.725	0.000	0.755	1.325
Expert	0.477	0.099	4.798	0.000	0.560	1.785
R^2= 0.475 Adj R^2 =0.448						
F= 17.216 Sig= 0 .000						

ويلاحظ الباحثان تعليقاً على الجدول رقم (15) السابق ما يلي:

بلغت قيمة Adjusted R^2 (0.448) وذلك يعني أن النموذج أن النموذج وما إشتمل عليه من متغيرات يمكنه تفسير 44.8% من التغير الكلى فى قيمة المتغير التابع (نغمة الإفصاح

DISC_TONE)، وباقى النسبة قد ترجع إلى عدم إدراج بعض المتغيرات المستقلة الأخرى ذات التأثير، أو إلى الخطأ العشوائى. أوضحت نتائج إختبار (VIF) لإختبار مشكلة الإزدواج الخطي في نموذج الإنحدار، أن قيمة (VIF) أقل من (10)، بما يُشير إلى أن نموذج الإنحدار لا يعانى من مشكلة الإزدواج الخطى (Sekaran and Bougie 2016).

يوضح الجدول رقم (15) السابق وجود تأثير إيجابي غير معنوى للسيكوباتية (PSYC) كأحد أبعاد الثالوث المظلم للشخصية على نغمة الإفصاح الإيجابية عن مخاطر الأمن السيبراني. تلك النتائج تتعارض مع بعض الخصائص المرتبطة بالسيكوباتيين، مثل الترويج الذاتي والإهتمام بالسمعة (Maasberg et al. 2020). يرى الباحثان أن تلك النتيجة ربما ترجع أيضاً لإنخفاض المستوى العام للسيكوباتية الشخصية لدى أفراد العينة، لذلك لم تظهر أية آثار سلبية على نغمة الإفصاح. **بناءً على ذلك سيتم رفض الفرض الفرعي (H32).**

وفيما يخص المتغيرات الرقابية، يُلاحظ وجود تأثير سلبي لكلٍ من (العمر Age، المؤهل العلمى Qualifications) على نغمة الإفصاح الإيجابية عن مخاطر الأمن السيبراني، وذلك عند مستوى معنوية أقل من (1%). بينما يوجد تأثير إيجابي لسنوات الخبرة (Expert) على نغمة الإفصاح الإيجابية عن مخاطر الأمن السيبراني، وذلك عند مستوى معنوية أقل من (1%). فى حين يوجد تأثير سلبي غير معنوى للنوع (Gender) على نغمة الإفصاح الإيجابية عن مخاطر الأمن السيبراني.

الفرض الفرعى الثالث (H33): يوجد تأثير إيجابي معنوي للسيكوباتية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على إحتمالية التلاعب بالمعلومات المرتبطة بمخاطر الأمن السيبراني. لاختبار هذا الفرض، سيتم تشغيل نموذج الإنحدار التالي بطريقة المربعات الصغرى:

$$DISC\_MANIP = B_0 + B_1\ PSYC + B_2\ Gender + B_3\ Age + B_4\ Qualification + B_5\ Expert + \varepsilon \quad (9)$$

يوضح الجدول رقم (16) نتائج تشغيل نموذج الانحدار رقم (9).

جدول 16: نتائج تحليل نموذج الانحدار رقم (9)

Variables	β	Std.Error	t	Sig	Collinearity statistics	
					Tolerance	VIF
Constant	5.477	1.014	5.403	0.000	-	-
PSYC	0.016	0.217	0.073	0.942	0.666	1.502
Gender	-1.606	0.436	-3.681	0.000	0.889	1.124
Age	-0.300	0.186	-1.614	0.110	0.602	1.660
Qualification	-0.440	0.148	-2.975	0.004	0.755	1.325
Expert	0.357	0.124	2.885	0.005	0.560	1.785
R^2= 0.293 Adj R^2 =0.256						
F= 7.866 Sig= 0 .000						

ويلاحظ الباحثان تعليقاً على الجدول رقم (16) السابق ما يلي:

بلغت قيمة Adjusted R^2 (0.256)، وذلك يعني أن النموذج وما إشتمل عليه من متغيرات يمكنه تفسير 25.6% من التغير الكلى فى قيمة المتغير التابع (التلاعب بالإفصاح DISC_MANIP)، وباقى النسبة قد ترجع إلى عدم إدراج بعض المتغيرات المستقلة الأخرى ذات التأثير، أو إلى الخطأ العشوائى. أوضحت نتائج إختبار (VIF) لإختبار مشكلة الإزدواج الخطي في نموذج الإنحدار، أن قيمة (VIF) أقل من (10)، بما يُشير إلى أن نموذج الإنحدار لا يعانى من مشكلة الإزدواج الخطى (Sekaran and Bougie 2016).

يوضح الجدول رقم (16) السابق وجود تأثير إيجابي غير معنوى للسيكوباتية كأحد أبعاد الثالوث المظلم للشخصية على إحتمالية التلاعب بالمعلومات المرتبطة بمخاطر الأمن السيبراني. تلك النتيجة تتعارض مع نتائج بعض الدراسات السابقة في مجال السيكوباتية، والتي تؤكد على تزايد إحتمالية تورط السيكوباتيون في ممارسات التلاعب والغش والممارسات غير الأخلاقية (Marshall et al. 2015; Bailey 2017; Harrison et al. 2018). يرى الباحثان أن تلك النتيجة ترجع لإنخفاض المستوى العام للسيكوباتية الشخصية لدى أفراد العينة، لذلك لم تظهر أية آثار سلبية على متغير التلاعب في الإفصاح عن مخاطر الأمن السيبراني. **بناءً على ذلك سوف يتم رفض الفرض الفرعي (H33).**

بخصوص المتغيرات الرقابية، يُلاحظ وجود تأثير سلبي لكلٍ من (النوع Gender، المؤهل العلمىQualifications) على إحتمالية التلاعب بالمعلومات المرتبطة بمخاطر الأمن السيبراني،

وذلك عند مستوى معنوية أقل من (1%). بينما يوجد تأثير إيجابي لسنوات الخبرة (Expert) على إحتمالية التلاعب بالمعلومات المرتبطة بمخاطر الأمن السيبراني، وذلك عند مستوى معنوية أقل من (1%). فى حين يوجد تأثير سلبي غير معنوى للعمر (Age) على إحتمالية التلاعب بالمعلومات المرتبطة بمخاطر الأمن السيبرانى.

فى ضوء نتائج اختبار الفروض الفرعية الثلاث السابقة، **سيتم رفض الفرض الرئيس الثالث (H3) القائل بوجود تأثير إيجابي معنوي للسيكوباتية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على اتجاهاتهم نحو الإفصاح عن مخاطر الأمن السيبراني.**

وتتعارض تلك النتائج مع ما توصلت إليه بعض الدراسات السابقة (Glenn et al. 2010; Bailey 2017; Hare 1991; Fehr et al. 1992; Patrick 2007; Bailey 2017; Harrison et al. 2018) ؛ التى أكدت على أن السيكوباتية هي أكثر سمة سلبية للثالوث المظلم مقارنة بالميكافيللية والنرجيسية. وترجع هذه النتائج لإنخفاض المستوى العام للسيكوباتية الشخصية لدى أفراد العينة في دراستنا، وهو ما سبق الإشارة إليه في تحليل One Sample t-test، حيث إنخفض مستوى السيكوباتية بشكل معنوي عن القيمة المحايدة "3"، وذلك يتوافق مع تأكيد بعض الباحثين على أن الآثار السلبية للثالوث المظلم تظهر فقط في المستويات العليا (Amernic and Craig 2010; Murphy 2012; Rijsenbilt and Commandeur 2013).

6- الخلاصة والنتائج والتوصيات

يتمثل الهدف الرئيس لهذه الدراسة في قياس أثر الثالوث المظلم كسمات شخصية على اتجاهات المحاسبين نحو الإفصاح عن مخاطر الأمن السيبراني. ولتحقيق الهدف الرئيس للدراسة قام الباحثان بدراسة شبه تجريبية على عينة من المحاسبين العاملين لدى بعض البنوك الكبرى في جمهورية مصر العربية، وقد بلغ حجم العينة النهائي 101 محاسب. وقد تم صياغة حالة عملية على أحد البنوك المصرية، وقد طلبنا من المحاسبين قراءة الحالة والإجابة على الأسئلة المرفقة بها والتي إشتملت على مجموعتين من الأسئلة لقياس المتغيرات البحثية. إشتملت المجموعة الأولى من الأسئلة على 9 أسئلة، قمنا من خلالها بقياس مدى قبول المحاسبين للإفصاح عن مخاطر الأمن السيبراني، ومدى إعتمادهم على النغمة الإيجابية للإفصاح، وأخيراً إحتمالية التلاعب في الإفصاح عن مخاطر الأمن السيبراني. إشتملت المجموعة الثانية على 27 سؤال، بواقع 9 أسئلة لقياس كل بُعد من أبعاد الثالوث المظلم في شخصية المحاسبين، تمثلت تلك الأبعاد في الميكافيللية،

والنرجسية، والسيكوباتية. وقد قام الباحثان بصياغة ثلاث فروض رئيسة للدراسة تم إختبارها بالإعتماد على أساليب الإحصاء الوصفي والإنحدار الخطي بطريقة المربعات الصغرى.

وقد تم قبول الفرض الرئيس الأول (H1) والخاص بوجود تأثير إيجابي معنوي للميكافيللية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على اتجاهاتهم نحو الإفصاح عن مخاطر الأمن السيبراني، حيث لاحظ الباحثان تزايد درجة قبول الميكافيليون للإفصاح عن المخاطر الأمن السيبراني، فى محاولة لاستغلال هذا النوع من الإفصاح لتحقيق الترويج الذاتي Self– promotion، وتحقيق رؤيتهم الاستراتيجية (Bailey 2015; Maasberg et al. 2020). اتضح ذلك عند فحص أثر الميكافيللية على النغمة الإيجابية للإفصاح، حيث لاحظ الباحثان تزايد توجه الميكافيليون لقبول النغمة الإيجابية للإفصاح، كذلك لاحظنا تزايد إحتمالية تلاعب الميكافيليون بالمعلومات المرتبطة بالإفصاح عن مخاطر الأمن السيبراني وتحايلهم من أجل عدم الإفصاح عن المخاطر قدر الإمكان، وتجنب الإفصاح عن محاولات الإختراق السابقة أو المحتملة، وقد جاءت جميع النتائج معنوية عند مستوى أقل من (1%).

كما تم قبول الفرض الرئيس الثاني (H2) والخاص بوجود تأثير إيجابي معنوي للنرجسية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على اتجاهاتهم نحو الإفصاح عن مخاطر الأمن السيبراني، حيث لاحظ الباحثان تزايد درجة قبول النرجسيون للإفصاح عن مخاطر الأمن السيبرانى، وهذا ربما يرجع لقدرتهم على إستغلال هذا النوع من الإفصاح للحصول على الثناء المتكرر والإعجاب، ودعم صورتهم الذاتية الرائعة، ودعم الأنا "Ego" (Lassoued and Khanchel 2022). وهو ما اتضح من نتائج الإختبارات التالية التي أكدت على توجه النرجسيون لتبني النغمة الإيجابية للإفصاح عن مخاطر الأمن السيبراني، كما لاحظنا تزايد إحتمالية تلاعب النرجسيون بالمعلومات المرتبطة بمخاطر الأمن السيبراني وتحايلهم من أجل عدم الإفصاح عن المخاطر قدر الإمكان، وتجنب الإفصاح عن محاولات الإختراق السابقة أو المحتملة، وقد جاءت جميع النتائج معنوية عند مستوى أقل من (1%).

أخيراً تم رفض الفرض الرئيس الثالث (H3) والخاص بوجود تأثير إيجابي معنوي للسيكوباتية كسمة شخصية للمحاسبين في البنوك العاملة في مصر على اتجاهاتهم نحو الإفصاح عن مخاطر الأمن السيبراني، حيث لاحظ الباحثان عدم وجود تأثير معنوي للسيكوباتية على مدى قبول المحاسبون للإفصاح عن مخاطر الأمن السيبراني، أو النغمة الإيجابية للإفصاح، أو التلاعب بالمعلومات المرتبطة بالإفصاح عن مخاطر الأمن السيبراني. وترجع تلك النتيجة من وجة نظرنا

لإنخفاض مستوى السيكوباتية لدى أفراد العينة، فقد كان المتوسط العام لمؤشر السيكوباتية أقل من القيمة المحايدة "3" وذلك عند مستوى معنوية أقل من (1%). ويبدو هذا التفسير منطقياً، حيث تظهر الآثار السلبية للثالوث المظلم فقط في المستويات العليا (e.g.,Murphy 2012;Rijsenbilt and Commandeur 2013). وبناءً على ذلك فإن رفض الفرض الثالث قد جاء نتيجة ظروف العينة التي إعتمد عليها الباحثان.

في ضوء ما تقدم يوصي الباحثان بما يلي:

- يجب إدخال بعض الاختبارات الشخصية والنفسية على متخذى القرارات في الإدارات العليا في منشآت الأعمال، والمتابعة المستمرة لنتائج تلك الإختبارات لمعالجة المستويات المتطرفة لأى سمة من السمات المظلمة حتى لا تؤذي تلك السمات بيئة العمل داخل المنشآت.
- نقترح تدريس مقرر لتعريف طلاب المحاسبة بالإنعكاسات المحتملة للثالوث المظلم كسمات شخصية للإدارة والمحاسبين على جودة التقارير المالية وجودة عملية المراجعة.
- نقترح على البنوك الإستعانة ببعض المختصين فى دراسة السمات الشخصية والنفسية لتدريب العاملين على التعامل بشكل إيجابي مع السمات الشخصية المظلمة لتجنب الآثار السلبية لتلك السمات على عملية إتخاذ القرار.
- يجب تنظيم الإفصاح عن مخاطر الأمن السيبراني في بيئة الأعمال المصرية، مع ضرورة تبني إطاراً موحداً للإفصاح بين المنشآت في السوق.
- يجب أن تُلزم الجهات التنظيمية الإدارة بتقديم إقرار بأن المعلومات التي تم الإفصاح عنها في تقرير الأمن السيبراني صحيحة، ومكتملة، ولم يتم إخفاء أية معلومات جوهرية عن مخاطر الأمن السيبراني. ولعل أرفاق تقرير بمراجعتها بها يكون مفيداً.
- يجب على الجهات التنظيمية التوجه نحو إلزام مراقبي الحسابات بمراجعة معلومات مخاطر الأمن السيبراني، التي توفرها المنشآت لإضفاء مزيداً من المصداقية عليها.

7- مقترحات لدراسات مستقبلية

يقترح الباحثان العديد من الدراسات المستقبلية في البيئة المصرية امتداداً لهذه الدراسة؛ ومنها ما يلي:

- قياس أثر الثالوث المظلم كسمات شخصية للإدارة على ممارسات إدارة الأرباح.
- قياس أثر الثالوث المظلم كسمات شخصية للإدارة على ممارسات الغش المحاسبي.
- قياس أثر الثالوث المظلم كسمات شخصية للإدارة على ممارسات التجنب الضريبي.
- قياس أثر الثالوث المظلم كسمات شخصية للإدارة على أتعاب عملية المراجعة.

- قياس أثر الثالوث المظلم كسمات شخصية للإدارة على قابلية القراءة Readability لتقارير مخاطر الأمن السيبراني.
- قياس أثر الثالوث المظلم كسمات شخصية للإدارة على المحتوى الإعلامي لتقارير مخاطر الأمن السيبراني.
- قياس أثر حوكمة الشركات على العلاقة بين الثالوث المظلم كسمات شخصية للإدارة والمحتوى الإعلامي لتقارير مخاطر الأمن السيبراني.

المراجع

أولاً: المراجع باللغة العربية

الاستراتيجية الوطنية للأمن السيبراني. (2017–2021). المجلس الأعلى للأمن السيبراني. رئاسة مجلس الوزراء، جمهورية مصر العربية.

السمحان، منى عبد الله. (2020). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. ***مجلة كلية التربية، جامعة المنصورة***، العدد 111، ص54–95.

جمعية الطب النفسي الأمريكية. (2004). ***المرجع السريع إلى الدليل التشخيصي والإحصائي الرابع المعدل للاضطرابات النفسية***. ترجمة د. تيسير حسون. دمشق مستشفى ابن سينا.

محمد، عبد الناصر طه إبراهيم. (2021). الميكافيللية وعلاقتها بالسلوكيات غير الأخلاقية الموالية للتنظيم: دراسة تحليلية لدور بعض المتغيرات التفاعلية. ***المجلة العلمية للدراسات والبحوث المالية والتجارية. كلية التجارة، جامعة دمياط***، العدد الثاني، الجزء الثالث، يوليو، ص1–53.

هيئة السوق المالية السعودية. (2019). ***الدليل الإسترشادي للأمن السيبراني لمؤسسات السوق المالية***. هيئة السوق المالية السعودية.

ثانياً: المراجع باللغة الأجنبية

Abraham, C., Chatterjee, D., andSims. R. R. (2019). Muddling through cybersecurity: Insights from the US healthcare industry. ***Business Horizons***, Vol. 62, No. 4, pp. 539–548.

AICPA. (2017a). Description criteria for management's description of an entity's cybersecurity risk management program, ***American Institute of Certified Public Accountants (AICPA),*** Assurance Services Executive Committee, New York, NY.

AICPA. (2017b). Reporting on an entity's cybersecurity risk management program and controls—attestation guide. ***American Institute of Certified Public Accountants***, New York, NY: AIPCA.

AICPA. (2017c). AICPA unveils cybersecurity risk management reporting framework. ***American Institute of Certified Public Accountants***, Available at:https://www.aicpa.org/news/article/aicpa-unveils-cybersecurity-risk-management-reporting-frame-work

Amernic, J. H. and Craig, R. J. (2010). Accounting as a facilitator of extreme narcissism. ***Journal of Business Ethics***, Vol. 96, pp. 79-93.

Amoroso, E. (2006). ***Cyber Security***. New Jersey: Silicon Press.

Ashraf, M. (2020). The role of market forces and regulation in disclosure: Evidence from cyber risk factors, Doctoral dissertation, The University of Arizona.

Babiak, P., and Hare, R. (2006). ***Snakes in suits: When psychopaths go to work***. Regan Books.

Bailey, C. D. (2015). Psychopathy, academic accountants' attitudes toward unethical research practices, and publication success. ***The Accounting Review***, Vol. 90, No. 4, pp. 1307-1332.

Bailey, C. D. (2017). Psychopathy and accounting students' attitudes towards unethical professional practices. ***Journal of Accounting Education***, Vol. 41, pp. 15–32.

Boddy, C. R. (2015). Organizational psychopaths: a ten year update.***Management Decision***, Vol. 53, pp. 2407-2432.

Brody, R. G., Melendy, S. R., and Perri, F. S. (2012). Commentary from the American accounting association's 2011 annual meeting panel on emerging issues in fraud research.***Accounting Horizons***, Vol. 26, pp. 513-531.

Buchholz, F., Lopatta, K., and Maas, K. (2019). The deliberate engagement of narcissistic CEOs in earnings management. ***Journal of Business Ethics***, Vol. 167, pp. 663–686.

Buss, D. M., and Shackelford, T. K. (1997). Susceptibility to infidelity in the first year of marriage. ***Journal of Research in Personality***, Vol. 31, No. 2, pp.193–221.

Campbell, W. K., Bonacci, A. M., Shelton, J., Exline, J. J., and Bushman, B. J. (2004). Psychological entitlement: Interpersonal consequences and validation of a self-report measure. ***Journal of Personality Assessment***, Vol. 83, No. 1; pp. 29–45.

Capalbo, F., Frino, A., Lim, M. Y., Mollica, V., and Palumbo, R. (2018). The impact of CEO narcissism on earnings management. ***Abacus***, Vol. 54, No. 2, pp. 210–226.

Center for Audit Quality. (2016). 2016 main street investor survey. Available at: https://www.thecaq.org/2016-main-street-investor-survey.

Chatterjee, A., and Hambrick, D. C. (2007). It's all about me: Narcissistic chief executive officers and their effects on company strategy and performance. ***Administrative Science Quarterly***, Vol. 52, 351–386.

Chatterjee, A., and Pollock, T. (2016). Master of puppets: How narcissistic CEOs construct their professional worlds. ***Academy of Management Review***, Vol. 42, pp. 703–725.

Christie, R., and Geis, F. (1970). Implications and speculations. In R. Christie and F. Geis (Eds.), ***Studies in Machiavellianism*** (pp. 339–358). Academic Press.

Clarke, J. (2005). ***Working with Monsters: How to Identify and Protect Yourself from the Workplace Psychopath***, Random House, Sydney.

Cohen, J., Ding, Y., Lesage. C., and Stolowy, H. (2010). Corporate fraud and managers' behavior: Evidence from the press. ***Journal of Business Ethics***, Vol.95,pp. 271-315.

Cooper, S., and Peterson, C. (1980). Machiavellianism and spontaneous cheating in competition. ***Journal of Research in Personality***, Vol. 14, pp. 70–75.

Corry, N., Merritt, R. D., Mrug, S., and Pamp, B. (2008). The factor structure of the narcissistic personality inventory. ***Journal of Personality Assessment***, Vol. 90, pp. 593–600.

Cressey, D. (1973). ***Other people's money***. Patterson Smith.

CSA .(2017). Multilateral Staff Notice 51-347: Disclosure of cyber security risks and incidents. ***Canadian Securities Administrator***, January 19,40 OSCB 605.

Dahling, J. J., Whitaker, B. G., and Levy, P. E. (2009). The development and validation of a new machiavellianism scale. ***Journal of Management***, Vol. 35, pp. 219-257.

Dakin, R. (2012). SEC cyber risk disclosure guidance. Available at: https://www.omegasecure.com/wp-content/uploads/2016/03/Coalfire-Perspective-SEC-Cyber-Risk-Disclosure-Guidance.pdf

Daugherty, B., Dickins, D., Hatfield, R., and Higgs, J. (2012). An examination of partner perceptions of partner rotation: Direct and indirect consequences to audit quality. Auditing: A Journal of Practice and Theory, Vol. 31, No. 1, pp. 97–114.

Davies, P. J. (2020). How wirecard went from tech star to bankrupt. Available at: https://www.wsj.com/articles/wirecard-bankruptcy-scandal-missing-$2billion-11593703379

Deumes, R., and Knechel, W. R. (2008). Economic incentives for voluntary reporting on internal risk management and control systems. ***Auditing: A Journal of Practice and Theory,*** Vol. 27, No. 1, pp. 35–66.

Domino, M. A., Wingreen, S. C. and Blanton, J. E. (2015). Social cognitive theory: The antecedents and effects of ethical climate fit on organizational attitudes of corporate accounting professionals—A reflection of client narcissism and fraud attitude risk. ***Journal of Business Ethics***, Vol. 131, pp.453-467.

Dorminey, J., Fleming, A. S., Kranacher, M-J., and Riley, R. A. (2012). The evolution of fraud theory. ***Issues in Accounting Education***, Vol. 27, pp. 555–579.

Ebaid, I. E. S. (2016). International accounting standards and accounting quality in code-law countries: The case of Egypt. ***Journal of Financial Regulation and Compliance***, Vol. 24 No. 1, pp. 41-59.

Ettredge, M. L., and Richardson, V. J. (2003). Information transfer among internet firms: The case of hacker attacks. ***Journal of Information Systems***, Vol. 17, No. 2, pp.71–82.

Fehr, B., Samsom, D., and Paulhus, D. L. (1992). The construct of machiavellianism: Twenty years later. In Spielberger, C. D. and Butcher, J. N. (Eds.), ***Advances in Personality Assessment***, Vol. 9, pp. 77-116.

Frank, M. L., Grenier, J. H., and Pyzoha, J. S. (2019). How disclosing a prior cyberattack influences the efficacy of cybersecurity risk management reporting and independent assurance. ***Journal of Information Systems***, Vol. 33, No. 3, pp. 183-200.

Furnham, A., Richards, S. C., and Paulhus, D. L. (2013). The dark triad of personality: A 10 year review. ***Social and Personality Psychology Compass***, Vol. 7, No. 3, pp. 199–216.

Glenn, A. L., Koleva, S., Iyer, R., Graham, J., and Ditto, P. H. (2010). Moral identity in psychopathy. ***Judgment and Decision Making***, Vol. 5, No. 7, pp. 497–505.

Gunnthorsdottir, A., McCabe, K., and Smith, V. (2002). Using the Machiavellianism instrument to predict trustworthiness in a bargaining game. ***Journal of Economic Psychology***, Vol. 23, No. 1, pp. 49–66.

Ham, C., Lang, M., Seybert, N., and Wang, S. (2017). CFO narcissism and financial reporting quality. ***Journal of Accounting Research***, Vol. 55, No. 5, pp. 1089–1135.

Ham, C., Seybert, N., and Wang, S. (2018). Narcissism is a bad sign: CEO signature size, investment, and performance. ***Review of Accounting Studies***, Vol. 23, pp. 234–264.

Hambrick, D. C., and Mason, P. A. (1984). Upper echelons: The organization as a re-flection of its top managers. ***Academy of Management Review***, Vol. 9, No.2, pp.193-206.

Hare, R. D. (1985). Comparison of procedures for the assessment of psychopathy. ***Journal of Consulting and Clinical Psychology***, Vol. 53, pp. 7–16.

Hare, R. D. (1991). ***Psychopathy Check List – Revised***. (2nd ed.). Toronto: Multi-Health Systems.

Harrison, A., Summers, J., andMennecke, B. (2018). The effects of the dark triad on unethical behavior. ***Journal of Business Ethics***, Vol. 153, pp. 53–77.

Heinle, M. S., and Smith, K. C. (2017). A theory of risk disclosure. ***Review of Accounting Studies***, Vol. 22, No. 4, pp. 1459-1491.

Hilary, G., Segal, B., and Zhang, M. H. (2016). Cyber-risk disclosure: who cares?. Georgetown McDonough School of Business Research Paper, (2852519).

https://www.nytimes.com/2018/03/05/business/dealbook/sec-cybersecurity-guidance.html

https://www.pwc.com/sg/en/publications/assets/gsiss-2018.pdf

IFAC. (1999). ***Enhancing Shareholder Wealth by Better Managing Business Risk***. International Federation of Accountants, Financial and Management Accounting Committee.

Johnson, E. N., Kuhn Jr, J. R., Apostolou, B. A., and Hassell, J. M. (2013). Auditor perceptions of client narcissism as a fraud attitude risk factor. Auditing: A Journal of Practice and Theory, Vol. 32, No. 1, pp. 203-219.

Jonason, P. K., Slomski, S., and Partyka, J. (2012). The dark triad at work: How toxic employees get their way. ***Personality and Individual Differences***, Vol. 52, No. 3, pp. 449–453.

Jones, D. N., and Paulhus, D. L. (2011). The role of impulsivity in the dark triad of personality. ***Personality and Individual Differences***, Vol. 51, No. 5, pp. 679–682.

Jones, D. N., and Paulhus, D. L. (2014). Introducing the Short Dark Triad (SD3). ***Assessment***, Vol. 21, No. 1, pp. 28–41.

Jorgensen, B. N., and Kirschenheiter, M. T. (2003). Discretionary risk disclosure. ***The Accounting Review***, Vol. 78, No. 2, pp. 449–469.

Kemmerer, R. A. (2003). Cybersecurity. Proceedings of the 25th IEEE, ***International Conference on Software Engineering***, pp.705-715.

Kirkman, C. A. (2005). From soap opera to science: towards gaining access to the psychopaths who live amongst us. ***Psychology and psychotherapy***, Vol. 78, pp. 379-396.

Lassoued, N., and Khanchel, I. (2022). Voluntary CSR disclosure and CEO narcissism: The moderating role of CEO duality and board gender diversity. ***Review of Managerial Science***, pp. 1-49.

Lilienfeld, S. O., and Andrews, B. P. (1996). Development and preliminary validation of a self-report measure of psychopathic personality traits in noncriminal population. ***Journal of Personality Assessment***, Vol. 66, pp. 488–524.

Ma, G. (2015). CEO narcissism and management forecasting. Working paper, NUS Business School, Singapore.

Maasberg, M., Van Slyke, C., Ellis, S., and Beebe, N. (2020). The dark triad and insider threats in cyber security. ***Communications of the ACM***, Vol. 63, No. 12, pp. 64-80.

Marquez-Illescas, G., Zebedee, A. A., and Zhou, L. (2019). Hear me write: Does CEO narcissism affect disclosure?. ***Journal of business ethics***, Vol. 159, No. 2, pp. 401-417.

Marshall, A. J., Ashleigh, M. J., Baden, D., Ojiako, U., andGuidi, M. G. D. (2015). Corporate psychopathy: Can 'search and destroy' and 'hearts and minds' military metaphors inspire HRM solutions?. ***Journal of Business Ethics***, Vol. 128, pp. 495–504.

Mashayekh, S., Habibzade, M., andHasanzadeKucho, M. (2021). The effect of CEO narcissism on voluntary disclosure. ***Accounting and Auditing Review***, Vol. 27, No. 4, pp. 649-671.

Masterson, J. D. (2015). Emerging SEC guidance and enforcement regarding data privacy and breach disclosures, Inside Counsel, available at; https://www.quarles.com/publications/emerging-sec-guidance-and-enforcement-regarding-data-privacy-and-breach-disclosures

Mautz, R. K., and Sharaf, H. A. (1961). ***The Philosophy of Auditing***. Madison, WI: American Accounting Association.

Menon, M. K., and Sharland, A. (2011). Narcissism, exploitative attitudes, and academic dishonesty: An exploratory investigation of reality versus myth. ***Journal of Education for Business***, Vol. 86, pp. 50–55.

Murphy, P. R. (2012). Attitude, machiavellianism and the rationalization of misreporting. ***Accounting, Organizations and Society***, Vol. 37, pp. 242–259.

Mutschmann, M., Hasso, T., and Pelster, M. (2021). Dark triad managerial personality and financial reporting manipulation. ***Journal of Business Ethics***, pp. 1-26.

Newman, C.A. 2018. When to report a cyberattack? For companies, that's still a dilemma. Available at:

O'Reilly, C. A., Doerr, B., Caldwell, D. F., and Chatman, J. A. (2013). Narcissistic CEOs and Executive Compensation. ***The Leadership Quarterly***, pp.1-13.

Olsen, K. J., andStekelberg, J. M. (2016). CEO narcissism and corporate tax sheltering. ***Journal of American Taxation Association***, Vol. 38, pp. 1–42.

Olsen, K. J., Dworkis, K. K., and Young, S. M. (2014). CEO narcissism and accounting: A picture of profits. ***Journal of Management Accounting Research***, Vol. 26, pp. 243–267.

Patrick, C. J. (2007). Antisocial personality disorder and psychopathy. In O'Donohue, W. T., Fowler, K. A., and Lilienfeld, S. O. (Eds.), ***Personality disorders: toward the DSM-V***. SAGE.

Paulhus, D. L., and Jones, D. N. (2015). Measures of dark personalities. In G. Boyle, D. Saklofske, and Matthews, G. (Eds.), ***Measures of personality and social psychological constructs*** (1st ed., pp. 562–594). Academic Press.

Paulhus, D. L., and Williams, K. M. (2002). The dark triad of personality: Narcissism, machiavellianism, and psychopathy. ***Journal of Research in Personality***, Vol. 36, pp. 556–563.

Perols, R. R. (2019). Two essays on the impact of cybersecurity risk management examinations on investor perceptions and decisions. Graduate Theses and Dissertations.

PwC. (2017). The US supplement to PwC's annual global CEO survey. 20th CEO survey, available at: https://www.pwc.com/gx/en/ceo-survey/pdf/20th-global-ceo-survey-us-supplement-executive-dialogues.pdf

PwC. (2018). The global state of information security® survey 2018. Price Waterhouse Coopers. Available at:

Ramamoorti, S. (2008). The Psychology and sociology of fraud: Integrating the behavioral sciences component into fraud and forensic accounting curricula. ***Issues in Accounting Education***, Vol. 23, No. 4, pp. 521-533.

Raskin, R., and Shaw, R. (1988). Narcissism and the use of personal pronouns. ***Journal of Personality***, Vol. 56, pp. 393–404.

Rauthmann, J. F., and Kolar, G. P. (2012). How "dark" are the dark triad traits? examining the perceived darkness of narcissism, machiavellianism, and psychopathy. ***Personality and Individual Differences***, Vol. 53, pp. 884–889.

Ray, J. J., and Ray, J. A. B. (1982). Some apparent advantages of subclinical psychopathy. ***Journal of Social Psychology***, Vol. 117, pp. 135-142.

Rijsenbilt, A., and Commandeur, H. (2013). Narcissus enters the courtroom: CEO narcissism and fraud. ***Journal of Business Ethics***, Vol.117, pp. 413–429.

Schlenker, B. R. (2008). Integrity and character: Implications of principled and expedient ethical ideologies. ***Journal of Social and Clinical Psychology***,Vol. 27, No. 10, pp. 1078–1125.

SEC. (2011). CF disclosure guidance: Topic No. 2 cybersecurity. Washing-ton, DC. Retrieved from: https://www.sec.gov/divisions/ corpfin /guidance/cfguidance-topic2.htm

SEC. (2018). Commission statement and guidance on public company cybersecurity disclosures. Washington DC Retrieved from: https://www.sec.gov/rules/interp/2018/33-10459.pdf

SEC. (2022). Cybersecurity risk management for investment advisers, registered investment companies, and business development

companies. Washington DC, Retrieved from: https://www.sec.gov/rules/proposed/2022/33-11028.pdf

Sekaran, U., and Bougie, R. (2016). ***Research Methods for Business: A Skill Building Approach***. 7th Edition. John Wiley & Sons.

Shafer, W. E., and Wang, Z. (2011). Effects of ethical context and machiavellianism on attitudes toward earnings management in China. ***Managerial auditing journal***, Vol. 26, No. 5, pp. 372-392.

Stevens, G. W., Deuling, J. K., and Armenakis, A. A. (2012). Successful psychopaths: Are they unethical decision-makers and why?. ***Journal of Business Ethics***, Vol. 105, pp. 139-149.

Trompeter, G. M., Carpenter, T.D., Desai, N., Jones, K. L., and Riley, R. (2012). A synthesis of fraud-related research. ***Auditing: A Journal of Practice and Theory***, Vol. 32, pp. 287–321.

Utami, I., Wijono, S., Noviyanti, S., and Mohamed, N. (2019). Fraud diamond, machiavellianism and fraud intention. ***International Journal of Ethics and Systems***, Vol. 35, No. 4, pp. 531-544.

Vladu, A. B. (2013). Machiavellianism and short-term earnings management practices. ***Annales Universitatis Apulensis: Series Oeconomica***, Vol. 15, No. 2, pp. 467-472.

Wang, T., Kannan, K. N., and Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. ***Information*** Systems Research, Vol. 24, No. (2): pp. 201–218.

World Economic Forum. (2019). Regional risks for doing business 2019. Insight report. Retrieved from Geneva, ***World Economic Forum***, 91-93 route de la Capite, CH-1223 Cologny/Geneva, Switzerland

Yang, L., Lau, L., and Gan, H. (2020). Investors' perceptions of the cybersecurity risk management reporting framework. ***International Journal of Accounting and Information Management***, Vol. 28 (1), pp. 167-183.

Young, S. M., Du, F., Dworkis, K., and Olsen, K. J. (2014). It's all about all of us–the rise of narcissism and its implications for management control system research. ***Journal of Management Accounting Research***, Vol. 28, pp. 1–44.

ملحق رقم (1)

الأستاذ الفاضل/الأستاذة الفاضلة

تحية طيبة وبعد....

يقوم الباحثان بإعداد دراسة بعنوان" **قياس أثر بعض السمات الشخصية للمحاسبين على جودة الإفصاح عن إدارة مخاطر الأمن السيبراني**".

مقدم لسيادتكم إحدى الحالات العلمية لأحد البنوك المصرية، لذا نرجو من سيادتكم التكرم بقراءة الحالة ثم الإجابة عن الأسئلة المرفقة، حيث تمثل آرائكم إضافة جوهرية للجانب الأكاديمي الذي يتناوله الباحثان. مؤكدين لسعادتكم على أن جميع الإجابات ستعامل بسرية تامة، وسيقتصر استخدامها على أغراض البحث العلمي فقط. وفي حالة رغبة سعادتكم في الحصول على النتائج نرجو منكم كتابة بريد الكتروني صالح حتى نتمكن من إرسال النتائج لسعادتكم.

نشكركم مقدماً على حُسن تعاونكم، ونتمنى لكم مزيداً من التقدم والرقي.

وتفضلوا بقبول فائق الإحترام والتقدير

الباحثان

د/عارف محمود كامل عيسى
أستاذ مساعد بقسم المحاسبة، كلية التجارة جامعة القاهرة
مُعار إلى كلية إدارة الأعمال جامعة المجمعة

د/ سمير إبراهيم عبد العظيم
مدرس بقسم المحاسبة، كلية التجارة جامعة بني سويف
مُعار إلى كلية إدارة الأعمال جامعة المجمعة

القسم الأول: بيانات شخصية.

القسم الثاني: أهم المصطلحات الواردة في الدراسة.

القسم الثالث: بيانات الدراسة التجريبية.

القسم الأول: بيانات شخصية:

1- الإسم (اختياري) .....

2- العمر:

أقل من 30 ☐ من 30-39 ☐ من 40-49 ☐ 50 سنة فأكثر ☐

3- النوع:

ذكر : ☐ أنثي : ☐

4- المؤهل العلمى:

بكالوريوس ☐ ماجستير ☐ دكتوراه ☐

5- عدد سنوات الخبرة:.....

أقل من 5 سنوات ☐ من 16-20 سنة ☐

من 5-10 سنوات ☐ أكثر من 20 سنة ☐

من 11-15 سنة ☐

القسم الثاني: أهم المصطلحات

- مخاطر الأمن السيبراني (Cybersecurity Risk): تشير مخاطر الأمن السيبراني إلى الخسائر المحتملة نتيجة الأحداث التي يقوم فيها فرد أو جهة غير مصرح لها بإختراق نظام المعلومات للمنشأة والحصول على وصول غير مصرح به إلى المعلومات المهمة.

- إدارة مخاطر الأمن السيبراني: مجموعة من السياسات والعمليات والضوابط المصممة لحماية المعلومات، والأنظمة من الأحداث الأمنية التي يمكن أن تعرض أهداف الأمن السيبراني للبنك للخطر، واكتشاف والإستجابة للأحداث الأمنية والحد من آثارها والتعافي من تلك الأحداث الأمنية التي لم يستطع البنك منعه في الوقت المناسب.

ثالثًا: بيانات الدراسة التجريبية:

بصفتك مديراً مالياً بأحد البنوك وقد توافرت لديك معلومات عن إدارة مخاطر الأمن السيبراني في البنك كما يلي:

تعرض البنك (X) في نهاية عام 2021 م لمحاولة إختراق من مهاجمين (قراصنة) لنظام البنك، ولم تسفر تلك المحاولات عن أية خسائر، وذلك بفضل الإستثمار في البنية التحتية والأنظمة الالكترونية المتطورة للحد من تلك المخاطر سواء كانت داخلية أو خارجية.

لدى البنك نظام جيد لإدارة مخاطر الأمن السيبراني، كذلك بدأت إدارة المخاطر بالبنك (X) بتنفيذ مجموعة من التحديثاتالمهمة للحد من مخاطر الأمن السيبراني خلال العام الحالي 2022 م، بشكل استباقي، من خلال تفعيل برنامج إدارة أمن المعلومات لدى البنك، وللحفاظ على مستوى التزام كامل لقواعد وتعليمات البنك المركزي المصري، يلتزم البنك بالمعايير والأنظمة الدولية المعتمدة لإدارة الأمن السيبراني مثل معيار آيزو 27001، وأنظمة بطاقات الدفع ومعايير أمن البيانات (PCI–DSS) وأنظمة التحويلات المالية الإلكترونية مثل؛ سويفت وخدمة سريع.

خلال الربع الأول من عام 2022 م، تم تطوير برنامج إدارة أمن المعلومات واستحداث الاستراتيجيات، والسياسات، وأنظمة الرقابة الداخلية اللازمة لدعم الكفاءة، والسرية، والنزاهة، في عمليات تكنولوجيا المعلومات في البنك وقدرات الرقابة، وتعزيز ثقة العملاء، والجهات الرقابية بشأن جودة الأمن السيبراني لدى البنك، الأمر الذي سُيساعد البنك على إدارة البيانات السرية وأصول تكنولوجيا المعلومات، كذلك يعتمد البنك على تمكين إدارة المخاطر من تنظيم البنية التحتية الإلكترونية للبنك، وتوسيع نطاق المقاييس الأمنية وتعزيزها في الأقسام التشغيلية المختلفةبما يحد من الآثار السلبية للهجمات الإلكترونية المحتملة سواء داخلية أو خارجية.

في ضوء ما تقدم أرجو إبداء رأيك في كل عبارة مما يلي:

	موافق تماماً 5	موافق 4	محايد 3	غير موافق 2	غير موافق 1 تماماً
قبول الإفصاح عن مخاطر الأمن السيبراني					
1- لا داعي للإفصاح عن محاولات الإختراق الداخلية أوالهجمات الإلكترونية الخارجية للأنظمة الإلكترونية للبنك، فتلك المعلومات حساسة ولا يجب أن يطلع عليها الأطراف الخارجية حتى لا يفقد البنك ثقة المستثمرين.					
2- يمتلك البنك الأدوات التي تمكنه من الحد من الخسائر المحتملة من مخاطر الأمن السيبراني سواء الناتجة عن الهجمات الداخلية أو محاولات الإختراق الخارجية. لذلك فلا داعي أن نفصح عن تلك المخاطر للمستثمرين.					
3- من وجهة نظري يجب التأكيد على جميع الأطراف المطلعة داخل البنك بعدم تسريب تلك المعلومات للأطراف الخارجية وإلا سيخضعون للعقوبات.					
نغمة الإفصاح					
4- في حالة وجود قواعد تلزم البنك بالإفصاح عن مخاطر الأمن السيبراني فإنه يجب الإشارة إلى الإجراءات التي إتخذها البنك في الآونة الأخيرة لدعم إدرة مخاطر الأمن السيبراني، دون الإشارة لأية هجمات سابقة أو محتملة.					
5- في حالة وجود قواعد تلزم البنك بالإفصاح عن مخاطر الأمن السيبراني فإننا سنركز على جميع الجوانب الإيجابية بشكل أكبر مع تجنب الإشارة للمشاكل التي يحملها نظام إدارة مخاطر الأمن السيبراني قدر الإمكان حتى نطمئن المستثمرين.					
6- على الرغم من أن الإفصاح عن الهجمات الخارجية أو محاولات الإختراق الداخلية قد تُعطي مؤشر عن مصداقيتنا في الإفصاح عن مخاطر الأمن السيبراني إلا أنها تُعرض البنك للعديد من المشاكل في أسواق المال، لذا فإنه من الأفضل التركيز على الجوانب الإيجابية وتجنب الجوانب السلبية قدر الإمكان.					

	موافق تماماً 5	موافق 4	محايد 3	غير موافق 2	غير موافق تماماً 1
التلاعب في الإفصاح					
7- نعتقد أن الخسائر الناتجة عن أية محاولة لإختراق أنظمة البنك أو الهجمات الالكترونية، يجب أن تعالج ضمن بند الخسائر المتنوعة دون الإفصاح عن تفاصيل تلك الخسائر في الإيضاحات المتممة حتى لا تُحدث تأثيراً سلبياً على أسعار الأسهم.					
8- في حالة وجود تأمين ضد مخاطر الأمن السيبراني لدى إحدى منشآت التأمين في هذه الحالة فلا داعي للإفصاح عن تلك الإختراقات سواء الفعلية أو المحتملة حتى لا يحدث تأثير سلبياً لأسعار الأسهم.					
9- في حالة وجود نص صريح ملزم في معايير المحاسبة للإفصاح عن الإختراقات السابقة والمحتملة للنظم الإلكترونية للبنك يجعلنا نبحث في صياغات تنقل للمستثمر الجوانب الإيجابية وتجنب الإفصاح عن الإختراقات السابقة قدر الإمكان.					

المجموعة الثانية من الأسئلة (السمات الشخصية للمحاسبين)

	موافق تماماً 5	موافق 4	محايد 3	غير موافق 2	غير موافق تماماً 1
الميكافيللية					
1- أؤمن بالحكمة التي تقول أنه يجب أن لا تخبر أحد بسرك.					
2- لا يوجد مانع لإستخدام بعض الحيل الذكية للوصول للأهداف.					
3- يجب أن يحيط المرء نفسه بأشخاص ذوي شأن.					
4- أتجنب دائماً مخالفة الآخرين لأنني قد أحتاجهم في المستقبل.					
5- من الحكمة أن نمتلك بعض المعلومات التي يمكن استخدامها ضد بعض الأفراد لاحقاً.					
6- على الفرد إنتظار الوقت المناسب للإنتقام من الآخرين.					
7- يجب أن نخفي بعض الأشياء عن الآخرين حفاظًا على السمعة.					
8- يجب على الفرد التأكد من أن خططه تفيد نفسه وليس الآخرين.					
9- غالبية الأفراد يمكن خداعهم.					

	موافق تماماً 5	موافق 4	محايد 3	غير موافق 2	غير موافق تماماً 1
النرجسية					
10- يراني الآخرون قائد بالفطرة.					
11- أكره أن أكون مركز إهتمام الآخرين (عكسي).					
12- العديد من الأنشطة الجماعية غالباً تكون مملة بدوني.					
13- أعلم أنني مميز لأن الجميع يخبروني بذلك بشكل مستمر.					
14- أميل إلى توسعة دائرة معارفي من الشخصيات المهمة.					
15- عندما أسمع مدح الآخرين اشعر بنوع من الإحراج. (عكسي).					
16- دائماً ما يتم وضعي في مقارنة مع شخصيات مشهورة.					
17- أرى نفسي شخصية عادية. (عكسي).					
18- عندى إصرار لنيل الإحترام الكافى الذى استحقه من الآخرين.					
السيكوباتية					
19- لدي قناعة بضرورة الإنتقام من السلطات (المسئولين).					
20- أتجنب المواقف ذات المخاطر العالية (عكسي).					
21- يجب أن يكون الإنتقام سريعاً وبشكل أسوء (البادئ أظلم).					
22- كثيراً ما يراني الآخرون أنني خارج نطاق السيطرة.					
23- لا مانع أن أكون لئيماً مع الآخرين.					
24- عادة ما يندم الأشخاص الذى يسيئون إلى.					
25- أحرص دائماً على الإلتزام بالقوانين، ولم أقع في مشاكل قانونية من قبل (عكسي).					
26- دائماً أتعامل بلطف مع الجنس الآخر وبصفة خاصة في اللقاء الأول.					
27- لا مانع من قول أي شيئ للحصول على ما أريد.					