المجلة العالمية للعلوم الشرعية والقانونية
الإصدار السابع والأربعون
المجلد (٦) العدد (٣)
٢٠٢٤ (١-١٤)

المجلة العالمية
للعلوم الشرعية والقانونية

Middle East Institution of scientific Publishing

استراتيجيات تعزيز الامن السيبراني في المؤسسات الصناعية ضمن اطار التحول الرقمي

فلاح بن شهاب بن فلاح الظفيري

نُشِرَ إلكترونياً في: ١٦ إبريل ٢٠٢٤م

*** مقدمة**

يجب على المؤسسات الصناعية اعتماد استراتيجية دفاعية متعمقة للأمن السيبراني، والتي تتضمن تنفيذ طبقات متعددة من الضوابط الأمنية للحماية من مجموعة واسعة من التهديدات السيبرانية حيث يشمل هذا النهج تجزئة الشبكة والتحكم في الوصول والتشفير وأنظمة كشف التسلل وحماية نقطة النهاية ومن خلال نشر مجموعة من التدابير الأمنية الوقائية والكشفية والتصحيحية، يمكن للمؤسسات إنشاء موقف دفاعي هائل يعالج نقاط الضعف المحتملة عبر بنيتها التحتية الرقمية، كما يعد إجراء تقييمات شاملة للمخاطر أمرًا بالغ الأهمية لتحديد مخاطر الأمن السيبراني وترتيب أولوياتها داخل المؤسسات الصناعية فتتضمن هذه التقييمات تقييم التأثير المحتمل للتهديدات السيبرانية على العمليات الحيوية، بالإضافة إلى تقييم فعالية الضوابط الأمنية الحالية ومن خلال فهم المخاطر المحددة التي تواجهها بيئات التكنولوجيا التشغيلية وتكنولوجيا المعلومات الخاصة بها، يمكن للمؤسسات تطوير تدابير أمنية مستهدفة للتخفيف من التهديدات ونقاط الضعف بشكل فعال(عبدالناصر محمد أيوب واخرون،2022) .

وفي سياق التحول الرقمي، يجب على المؤسسات الصناعية أن تتبنى نموذج أمان الثقة المعدومة، الذي يتحدى النهج الأمني التقليدي القائم على المحيط حيث تفترض Zero Trust وجود تهديدات داخل الشبكة وخارجها، وعلى هذا النحو، تتطلب التحقق الصارم من الهوية، والمراقبة المستمرة، وضوابط الوصول الصارمة من خلال تطبيق مبادئ الثقة المعدومة، يمكن للمؤسسات تقليل مخاطر الوصول غير المصرح به، والحركة الجانبية للتهديدات، وانتهاكات البيانات داخل شبكاتها الصناعية(نورهان صبحي محمد عطية, 2022).

ويظل الخطأ البشري أحد الأسباب الرئيسية لحوادث الأمن السيبراني في المؤسسات الصناعية. ولذلك، يجب على المؤسسات إعطاء الأولوية لتوعية الموظفين وبرامج التدريب لتعزيز ثقافة الوعي بالأمن السيبراني فيجب أن تغطي مبادرات التدريب أفضل الممارسات لتحديد التهديدات المحتملة والاستجابة لها، والتعرف على تكتيكات الهندسة الاجتماعية، وفهم أهمية الالتزام بالسياسات والإجراءات الأمنية ومن خلال تمكين الموظفين بالمعرفة والمهارات اللازمة للتعرف على المخاطر السيبرانية والتخفيف منها، يمكن للمؤسسات تعزيز وضعها الأمني بشكل كبير(Ncubukezi,2022) .

كما تعمل المؤسسات الصناعية ضمن قطاعات شديدة التنظيم، مثل الطاقة والتصنيع والبنية التحتية الحيوية فيعد الامتثال للوائح والمعايير الخاصة بالصناعة، مثل NIST SP 800-82 وIEC 62443 وISA/IEC 62443، أمرًا أساسيًا لضمان مرونة الأنظمة الرقمية والحفاظ على سلامة العمليات الصناعية، وإن الالتزام بهذه اللوائح لا يوضح الالتزام بأفضل ممارسات الأمن السيبراني فحسب، بل يساعد أيضًا المؤسسات على مواءمة جهودها الأمنية مع معايير الصناعة وإرشاداتها، لذا يعد التعاون بين المؤسسات الصناعية والوكالات الحكومية ومنظمات الأمن السيبراني فعالاً في مكافحة التهديدات السيبرانية ونقاط الضعف(عمار ياسر البابلي، 2021).

اولا: المشكلة البحثية

في سياق التحول الرقمي، تعد استراتيجيات تعزيز الأمن السيبراني داخل المؤسسات الصناعية أمرًا بالغ الأهمية لحماية البيانات والأنظمة الحساسة فلقد أدى دمج التقنيات الرقمية في العمليات الصناعية إلى ظهور نقاط ضعف جديدة، مما يجعل من الضروري تطوير استراتيجيات فعالة للأمن السيبراني مصممة خصيصًا لهذه البيئة، ويتضمن تعزيز الأمن السيبراني في المؤسسات الصناعية معالجة تحديات محددة تتعلق بتقارب التكنولوجيا التشغيلية (OT) وتكنولوجيا المعلومات (IT) ويوفر هذا التقارب مخاطر فريدة تتعلق بالأمن السيبراني وتتطلب أساليب متخصصة لحماية البنية التحتية الحيوية والعمليات الصناعية،

كما ويتطلب إطار التحول الرقمي اتباع نهج شامل للأمن السيبراني يشمل الاحتياجات والتحديات المحددة للمؤسسات الصناعية، ويشمل ذلك تنفيذ تدابير أمنية قوية لحماية الأنظمة والبيانات والأصول المادية المترابطة من التهديدات السيبرانية(عمار ياسر البابلي، 2021).

لذا تكمن مشكلة البحث في تحديد وتطوير استراتيجيات الأمن السيبراني المصممة خصيصًا والتي تخفف بشكل فعال من التهديدات السيبرانية المتطورة داخل المؤسسات الصناعية التي تمر بالتحول الرقمي وينطوي ذلك على معالجة نقاط الضعف والمخاطر المحددة المرتبطة بدمج التقنيات الرقمية في العمليات الصناعية، فضلا عن ضمان مرونة البنية التحتية الحيوية ضد الهجمات السيبرانية، ومما سبق يمكن صياغة الاسئلة البحثية في:-

١- ما هي الاعتبارات الأساسية المتعلقة بحوكمة الأمن السيبراني للمؤسسات الصناعية أثناء التحول الرقمي؟

٢- كيف يمكن للمؤسسات الصناعية ضمان العمليات الآمنة مع تعزيز الكفاءة والفعالية أثناء التحول الرقمي؟

٣- ما هي الثغرات الأمنية المحددة الأكثر صلة بالمؤسسات الصناعية في سياق التحول الرقمي؟

٤- ما هو الدور الذي تلعبه إدارة المعلومات في تعزيز الأمن السيبراني في إطار التحول الرقمي للمؤسسات الصناعية؟

٥- كيف يمكن تطبيق إطار الأمن السيبراني التابع للمعهد الوطني للمعايير والتكنولوجيا (NIST) لتطوير استراتيجية فعالة للأمن السيبراني للمؤسسات الصناعية في سياق التحول الرقمي؟

ثانيا: اهمية الدراسة

*** الأهمية العلمية**

١- يساهم البحث في الفهم العلمي لحوكمة الأمن السيبراني في سياق المؤسسات الصناعية التي تشهد التحول الرقمي، وتوسيع القاعدة المعرفية في هذا المجال.

٢- استكشاف مخاطر الأمن السيبراني الفريدة ونقاط الضعف التي يسببها التحول الرقمي، وتقديم رؤى حول تطوير استراتيجيات الأمن السيبراني المصممة خصيصًا للبيئات الصناعية.

*** الأهمية التطبيقية**

١- يقدم البحث استراتيجيات عملية لتعزيز الأمن السيبراني في المؤسسات الصناعية، ومعالجة احتياجات الشركات والمنظمات التي تسعى إلى تأمين عملياتها في العصر الرقمي بشكل مباشر.

٢- مساعدة المؤسسات الصناعية على تحسين دفاعات الأمن السيبراني لديها، وحماية البنية التحتية الحيوية، وحماية البيانات الحساسة من التهديدات السيبرانية.

٣- معالجة التحديات المحددة للأمن السيبراني في سياق التحول الرقمي، يساهم البحث في مرونة وأمن العمليات الصناعية، ودعم استمرارية وموثوقية الشركات في مواجهة التهديدات السيبرانية.

ثالثا: اهداف الدراسة

١- تسليط الضوء على أهمية حوكمة الأمن السيبراني في التحول الرقمي

٢- تحديد الثغرات الأمنية المحددة ذات الصلة بالمؤسسات الصناعية

٣- استكشاف دور المعلومات في التحول الرقمي في سياق المؤسسات الصناعية

٤- دراسة إطار الأمن السيبراني للمعهد الوطني للمعايير والتكنولوجيا (NIST)

٥- اقتراح استراتيجيات مؤسسية للأمن السيبراني في المؤسسات الصناعية

رابعا: منهجية الدراسة

سيستخدم البحث المنهج الوصفي لدراسة وتحليل تحديات واستراتيجيات الأمن السيبراني في سياق التحول الرقمي للمؤسسات الصناعية حيث يتضمن المنهج الوصفي مراقبة وتوثيق وتحليل الظواهر قيد الدراسة

خامسا: لمحة عامة عن التحول الرقمي في المؤسسات الصناعية

يشهد المشهد الصناعي تحولا عميقا مدفوعا بالتحول الرقمي، الذي يتميز بتقارب التقنيات المادية والرقمية. تستفيد المؤسسات الصناعية بشكل متزايد من الحلول الرقمية لتحسين عملياتها وتعزيز الإنتاجية والاستجابة لديناميكيات السوق المتغيرة فوفقًا لتقرير صادر عن مؤسسة البيانات الدولية (IDC)، من المتوقع أن يصل الإنفاق العالمي على التحول الرقمي إلى 2.3 تريليون دولار في عام 2023، مما يشير إلى اعتماد واسع النطاق للمبادرات الرقمية عبر الصناعات، وفي قلب التحول الرقمي في المنظمات الصناعية يكمن مفهوم الصناعة 4.0، الذي يشمل دمج الأنظمة المادية السيبرانية، وإنترنت الأشياء (IoT)، والحوسبة السحابية، والحوسبة المعرفية في عمليات التصنيع فوفقًا لدراسة أجرتها شركة Capgemini، تستثمر المنظمات الصناعية بكثافة في تقنيات الصناعة 4.0، حيث نفذت 87% من الشركات أو تخطط لتنفيذ مبادرات الصناعة 4.0 بحلول عام 2025(احمد مجر واخرون،2022) .

حيث أصبحت البيانات حجر الزاوية في التحول الرقمي في المنظمات الصناعية، مما يتيح اتخاذ القرارات

المستنيرة والتحليلات التنبؤية فتشير دراسة أجرتها شركة ديلويت إلى أن 67% من المديرين التنفيذيين في مجال التصنيع يعتقدون أن التحول الرقمي أدى إلى زيادة في استخدام تحليلات البيانات لدفع عمليات صنع القرار، مما يؤكد الدور المحوري للبيانات في تشكيل الاستراتيجيات الصناعية، ولقد أثرت مبادرات التحول الرقمي بشكل كبير على الكفاءة التشغيلية داخل المنظمات الصناعية كما وتسلط الأبحاث التي أجرتها شركة ماكينزي آند كومباني الضوء على أن التحول الرقمي يمكن أن يؤدي إلى زيادة بنسبة 20% إلى 30% في الكفاءة التشغيلية للمصنعين، مما يعرض الفوائد الملموسة للتدخلات الرقمية في تبسيط العمليات الصناعية (Cheng et al,2022).

ولقد أدى انتشار أجهزة إنترنت الأشياء وحلول الاتصال إلى إعادة تعريف العمليات الصناعية، مما يسهل المراقبة في الوقت الفعلي والصيانة التنبؤية وتحسين العمليات. فوفقًا لشركة Statista، من المتوقع أن يصل عدد أجهزة إنترنت الأشياء المتصلة المستخدمة في مختلف الصناعات إلى 30.9 مليار بحلول عام 2025، مما يعكس التكامل الشامل لتكنولوجيا إنترنت الأشياء في البيئات الصناعية، وتعتمد المنظمات الصناعية بشكل متزايد على الروبوتات المتقدمة والأتمتة لتعزيز الكفاءة والدقة في التصنيع والخدمات اللوجستية، ولقد أفاد الاتحاد الدولي للروبوتات أن تركيبات الروبوتات العالمية في قطاع التصنيع وصلت إلى 381 ألف وحدة في عام 2019، مما يؤكد الاعتماد المتزايد على الأنظمة الروبوتية لتحسين سير العمل الصناعي(ثاقب سعيد واخرون،2023) .

كما ولقد ظهر الذكاء الاصطناعي (AI) والتعلم الآلي (ML) كتقنيات تحويلية في البيئات الصناعية، مما يتيح الصيانة التنبؤية، ومراقبة الجودة، وتحسين العمليات حيث انه وفقاً لتقرير صادر عن مؤسسة جارتنر، قامت 37% من المؤسسات بتطبيق الذكاء الاصطناعي بشكل أو بآخر، كما شهدت التطبيقات الصناعية اعتماداً كبيراً، ومع تبني المنظمات الصناعية للتحول الرقمي، تصبح الحاجة إلى تدابير قوية للأمن السيبراني أمرًا بالغ الأهمية، وتسلط دراسة أجرتها شركة IBM الضوء على أن متوسط تكلفة اختراق البيانات للشركات الصناعية يبلغ 4.99 مليون دولار، مما يؤكد المخاطر المالية المرتبطة بالتهديدات السيبرانية وأهمية المرونة الرقمية في حماية العمليات الصناعية (نورهان صبحي محمد عطية،2022).

ويعمل التحول الرقمي على تمكين المؤسسات الصناعية من الابتكار وتقديم الحلول التي تركز على العملاء الأيونات. وجدت دراسة استقصائية أجرتها شركة Forrester Research أن 89% من قادة التصنيع يعتقدون أن التحول الرقمي أمر بالغ الأهمية لتحفيز الابتكار الذي يركز على العملاء، مما يسلط الضوء على الضرورة الاستراتيجية للاستفادة من القدرات الرقمية لتلبية احتياجات العملاء، فأصبح التقارب بين التقنيات الرقمية والاستدامة نقطة محورية للمنظمات الصناعية ويشير تقرير صادر عن المنتدى الاقتصادي العالمي إلى أن التحول الرقمي يمكن أن يتيح خفض انبعاثات الكربون العالمية بنسبة 15% بحلول عام 2030، مما يوفر فرصة مقنعة للمنظمات

الصناعية لمواءمة المبادرات الرقمية مع أهداف الاستدامة البيئية(بوحنية قوي،2023).

سادسا: أهمية الأمن السيبراني في عصر التحول الرقمي

لقد أدت رحلة التحول الرقمي إلى ظهور مشهد ديناميكي ومعقد للتهديدات السيبرانية فوفقًا لوكالة الأمن السيبراني وأمن البنية التحتية (CISA)، كانت هناك زيادة بنسبة 33٪ في حوادث برامج الفدية التي تستهدف أصول التكنولوجيا التشغيلية (OT) في عام 2020، مما يسلط الضوء على المخاطر السيبرانية المتصاعدة التي تواجهها المؤسسات التي تخضع للتحول الرقمي، وقد برزت خروقات البيانات باعتبارها خطرًا سائدًا في العصر الرقمي، مع ما يترتب على ذلك من آثار مالية كبيرة على المؤسسات كما كشف تقرير IBM لتكلفة خرق البيانات لعام 2021 أن متوسط التكلفة الإجمالية لخرق البيانات يبلغ 4.24 مليون دولار، مما يؤكد التأثير المالي الكبير لحوادث الأمن السيبراني على المؤسسات التي تتبنى التحول الرقمي(ماجده عبد الشافى محمد الهادى خالد،2023) .

وأصبح المشهد التنظيمي المحيط بحماية البيانات والخصوصية أكثر صرامة، مما يستلزم اتخاذ تدابير قوية للأمن السيبراني. فرضت اللائحة العامة لحماية البيانات (GDPR) للاتحاد الأوروبي غرامات يبلغ مجموعها 272.5 مليون يورو لعدم الامتثال منذ تطبيقها، مع التركيز على التداعيات القانونية والمالية لعدم كفاية الأمن السيبراني في العصر الرقمي، فيعد الأمن السيبراني جزءًا لا يتجزأ من بناء الثقة والحفاظ عليها في المجال الرقمي. كشفت دراسة أجرتها شركة برايس ووترهاوس كوبرز (PwC) أن 85% من المستهلكين لن يتعاملوا مع شركة ما إذا كانت لديهم مخاوف بشأن ممارساتها الأمنية، مما يؤكد العلاقة الحاسمة بين الأمن السيبراني وثقة العملاء وسمعة العلامة التجارية في العصر الرقمي (Saeed et al,2023).

بالاضافة الي ذلك تعتبر تدابير الأمن السيبراني ضرورية لضمان استمرارية الأعمال والمرونة التشغيلية في مواجهة التهديدات السيبرانية. وجد تقرير تكلفة خرق البيانات لعام 2020 الصادر عن معهد بونيمون أن المؤسسات التي لديها فريق استجابة للحوادث شهدت توفيرًا في التكلفة متوسطًا قدره 2 مليون دولار، مما يسلط الضوء على الدور الاستباقي للأمن السيبراني في تخفيف الخسائر المالية والاضطرابات التشغيلية (ناصر بن محمد بن عباس،2020).

ويستمر الاستثمار العالمي في حلول الأمن السيبراني في الارتفاع استجابة للتهديدات السيبرانية المتصاعدة فوفقًا لمؤسسة IDC، من المتوقع أن يتجاوز الإنفاق العالمي على المنتجات والخدمات المتعلقة بالأمن السيبراني 151.2 مليار دولار في عام 2023، مما يشير إلى الالتزام المالي الكبير بالتأهب للأمن السيبراني في العصر الرقمي، كما ويمثل النقص في المتخصصين في مجال الأمن السيبراني تحديًا كبيرًا للمؤسسات التي تتنقل في التحول الرقمي فقد سلط تقرير صادر عن (ISC)² الضوء على النقص العالمي في القوى العاملة البالغ 3.12 مليون متخصص في مجال الأمن السيبراني، وكشف عن الحاجة الملحة لتنمية المواهب وتوظيفها لمعالجة فجوة المهارات في

مجال الأمن السيبراني، حيث يعد الاستعداد للاستجابة لحوادث الأمن السيبراني أحد المحددات الرئيسية للمرونة التنظيمية. وجد تقرير هيسكوكس للجاهزية السيبرانية لعام 2021 أن 26% فقط من المؤسسات تعتبر خبراء في مجال السيبرانية، مما يشير إلى وجود فجوة سائدة في الاستعداد للاستجابة للحوادث ونضج الأمن السيبراني عبر الصناعات (Comizio et al,2016).

سابعا: الاستراتيجيات الحالية لتعزيز الأمن السيبراني في المؤسسات الصناعية

تواجه المؤسسات الصناعية مشهدًا ديناميكيًا ومتطورًا للتهديدات السيبرانية، والذي يتميز بانتشار برامج الفدية، وهجمات سلسلة التوريد، والتهديدات السيبرانية المادية المعقدة فوفقًا لتقرير التحقيقات في خروقات البيانات لعام 2021 الصادر عن شركة Verizon، فإن 29% من خروقات البيانات شملت قطاع التصنيع، مما يسلط الضوء على الطبيعة المنتشرة للتهديدات السيبرانية التي تستهدف المؤسسات الصناعية، ويمكن أن يكون لحوادث الأمن السيبراني آثار مالية وتشغيلية عميقة على المنظمات الصناعية ، ويتم التأكيد على ضرورة اتخاذ تدابير الأمن السيبراني المرنة من خلال أهمية العمليات الصناعية والعواقب المحتملة للاضطرابات السيبرانية(وفاء لطفى, 2022).

وتتبنى المنظمات الصناعية بشكل متزايد أطر ومعايير الأمن السيبراني لتوجيه مبادرات الأمن السيبراني الخاصة بها فيتم استخدام إطار عمل الأمن السيبراني NIST على نطاق واسع، حيث تطبق 50% من المؤسسات هذا الإطار، وفقًا لمسح أجراه معهد SANS، مما يسلط الضوء على انتشار أطر الأمن السيبراني المعترف بها في الصناعة في البيئات الصناعية، حيث تعد المراقبة المستمرة واكتشاف التهديدات من المكونات المحورية لاستراتيجيات الأمن السيبراني في المنظمات الصناعية فقد وجدت دراسة الكشف عن التهديدات التي أجراها معهد SANS أن 68% من المؤسسات تعتبر المراقبة المستمرة واكتشاف التهديدات هي التحكم الأمني الأكثر فعالية، مع التركيز على النهج الاستباقي لتحديد التهديدات السيبرانية والتخفيف من آثارها (Syafrizal et al,2020).

كما وتلعب برامج التدريب والتوعية في مجال الأمن السيبراني للموظفين دورًا محوريًا في تعزيز مرونة الأمن السيبراني في المنظمات الصناعية فوجدت دراسة أجرتها Cybersecurity Ventures أن 95% من جميع انتهاكات الأمن السيبراني ترجع إلى خطأ بشري، مما يؤكد الضرورة الاستراتيجية للاستثمار في تدريب الموظفين وتوعيتهم للتخفيف من المخاطر السيبرانية، حيث تقوم المنظمات الصناعية باستثمارات كبيرة في مجال الأمن السيبراني لتعزيز دفاعاتها ضد التهديدات السيبرانية فوفقًا لمؤسسة IDC، من المتوقع أن يتجاوز الإنفاق العالمي على المنتجات والخدمات المتعلقة بالأمن السيبراني 134 مليار دولار في عام 2022، مما يعكس الالتزام المالي الكبير بالتأهب للأمن السيبراني في البيئات الصناعية (He et al,2019).

ولقد اكتسب اعتماد الحلول الأمنية لإنترنت الأشياء الصناعي (IIoT) زخمًا داخل المؤسسات الصناعية ويتوقع تقرير صادر عن MarketsandMarkets أنه من المتوقع أن يصل سوق الأمن السيبراني الصناعي العالمي

إلى 22.8 مليار دولار بحلول عام 2023، مما يعكس التكامل الشامل لحلول أمان إنترنت الأشياء الصناعية في البيئات الصناعية(Syafrizal et al,2020).

ثامنا: تحديد الثغرات الأمنية المحددة في سياق التحول الرقمي

لقد أدت رحلة التحول الرقمي إلى ظهور مشهد ديناميكي ومعقد للتهديدات السيبرانية، مما يعرض المؤسسات لمجموعة من نقاط الضعف فوفقًا لتقرير التحقيقات في خرق البيانات لعام 2021 الصادر عن شركة Verizon، فإن 85% من الانتهاكات تضمنت استغلال نقاط الضعف المعروفة، مما يسلط الضوء على الطبيعة المنتشرة للثغرات الأمنية في سياق التحول الرقمي، كما يمكن أن يكون للثغرات الأمنية آثار مالية وتشغيلية كبيرة على المؤسسات التي تخضع للتحول الرقمي فوجد تقرير معهد بونيمون لتكلفة خرق البيانات لعام 2021 أن متوسط التكلفة الإجمالية لخرق البيانات للمؤسسات يبلغ 4.24 مليون دولار، مما يؤكد التأثير المالي الكبير للثغرات الأمنية على المؤسسات التي تتبنى المبادرات الرقمية(لمياء زواوي واخرون،2023) .

وتعد الإدارة الاستباقية للثغرات الأمنية أمرًا ضروريًا لتحديد وتخفيف الثغرات الأمنية في سياق التحول الرقمي، أبرزت دراسة أجرتها شركة IBM أن المؤسسات التي تحتوي على الاختراق في أقل من 30 يومًا توفر أكثر من مليون دولار أمريكي مقارنة بتلك التي تستغرق وقتًا أطول، مع التركيز على الفوائد المالية لإدارة الثغرات الأمنية الاستباقية في حماية المبادرات الرقمية، ايضا يؤدي انتشار أجهزة إنترنت الأشياء والتكنولوجيا التشغيلية في البيئات الصناعية والتشغيلية إلى ظهور ثغرات أمنية فريدة من نوعها، بما في ذلك اختطاف الأجهزة، ونقص التشفير، وإدارة الأجهزة غير الآمنة فوفقًا لتقرير تهديدات إنترنت الأشياء لعام 2021 الصادر عن F-Secure، شهدت أجهزة إنترنت الأشياء زيادة بنسبة 300% في الهجمات في النصف الأول من عام 2021، مما يسلط الضوء على تصاعد الثغرات الأمنية لإنترنت الأشياء في مشهد التحول الرقمي(هبة جمال الدين, 2023).

بالاضافة الي ذلك تشكل نقاط الضعف في سلسلة التوريد، بما في ذلك مخاطر الطرف الثالث، وهجمات سلسلة توريد البرامج، ونقاط ضعف البائعين، تهديدات كبيرة في سياق التحول الرقمي حيث وجد تقرير الأمن السيبراني لسلسلة التوريد لعام 2021 الصادر عن BlueVoyant أن 80% من المؤسسات تعرضت لهجوم على سلسلة توريد البرامج خلال الـ 12 شهرًا الماضية، مما يؤكد الطبيعة المنتشرة لثغرات أمان سلسلة التوريد(لمياء زواوي واخرون،2023).

ولا يزال استغلال نقاط الضعف المعروفة هو التكتيك السائد في الهجمات السيبرانية فوفقًا لتقرير اتجاهات الثغرات والتهديدات لعام 2021 الصادر عن NopSec، استفادت 60% من الانتهاكات من نقاط الضعف المعروفة، مما يؤكد أهمية إدارة الثغرات الاستباقية في التخفيف من التهديدات السيبرانية، ويمكن للمؤسسات التي تتمتع بإمكانات قوية للاستجابة للحوادث التخفيف من تأثير الثغرات الأمنية تقرير الاستعداد السيبراني لهيسكوكس وجدت دراسة عام 2021 أن 26% فقط من المؤسسات

تعتبر خبراء في مجال الأمن السيبراني، مما يشير إلى وجود فجوة سائدة في الاستعداد للاستجابة للحوادث ونضج الأمن السيبراني عبر الصناعات (هبة جمال الدين, 2023).

تاسعا: أطر وقوانين التي تحكم الأمن السيبراني في المؤسسات الصناعية

يُعرف إطار عمل الأمن السيبراني التابع للمعهد الوطني للمعايير والتكنولوجيا (NIST) على نطاق واسع بأنه دليل شامل لتحسين إدارة مخاطر الأمن السيبراني. وجدت دراسة أجراها معهد SANS أن 50% من المؤسسات قد نفذت إطار عمل الأمن السيبراني NIST، مما يعكس انتشاره كإطار أساسي لحوكمة الأمن السيبراني في البيئات الصناعيةن كما يوفر معيار ISO/IEC 27001 إطاراً معترفًا به عالميًا لأنظمة إدارة أمن المعلومات فووفقاً لمسح ISO، تم إصدار 47.054 شهادة لمعيار ISO/IEC 27001 عالمياً في عام 2020، مما يؤكد الاعتماد الواسع النطاق لهذا الإطار في مواءمة ممارسات الأمن السيبراني مع المعايير الدولية (Mirtsch et al,2020).

كما توفر ضوابط الأمان الحرجة لمركز أمن الإنترنت (CIS) مجموعة من الإجراءات ذات الأولوية للدفاع عن الأمن السيبراني. توصلت دراسة أجرتها CIS إلى أن المؤسسات التي تطبق أربعة على الأقل من ضوابط الأمن الحرجة الخاصة بـــ CIS يمكنها تقليل مخاطر الهجمات السيبرانية بنسبة تصل إلى 85%، مما يسلط الضوء على فعالية هذا الإطار في التخفيف من التهديدات السيبرانية، ايضا كان للقانون العام لحماية البيانات (GDPR) تأثير عميق على حماية البيانات والخصوصية للمؤسسات العاملة في الاتحاد الأوروبي وخارجه فأفاد المجلس الأوروبي لحماية البيانات أنه منذ تطبيق اللائحة العامة لحماية البيانات في عام 2018، تم فرض غرامات تزيد عن 272.5 مليون يورو بسبب عدم الامتثال، مما يؤكد المشهد التنظيمي الصارم الذي يحكم حماية البيانات (Li et al,2019).

وقد أنشأ قانون CCPA حقوقًا شاملة لخصوصية البيانات لسكان كاليفورنيا، مما يؤثر على ممارسات حماية البيانات في المؤسسات الصناعية فكشف تقرير صادر عن Truyo أن 75% من المؤسسات أجرت تغييرات على ممارسات خصوصية البيانات الخاصة بها استجابة لقانون CCPA، مما يسلط الضوء على التأثير التنظيمي لهذا القانون على إدارة البيانات الصناعية، كما تضع HIPAA المعيار لحماية بيانات المرضى الحساسة في قطاع الرعاية الصحية و أفاد مكتب وزارة الصحة والخدمات الإنسانية للحقوق المدنية أن التسويات والأحكام الصادرة عن HIPAA بلغت 14.8 مليون دولار في عام 2020، مما يؤكد التداعيات القانونية والمالية لعدم الامتثال للوائح HIPAA(محمد حسن عماد مكاوي, (2022).

وإن اعتماد أطر الأمن السيبراني واسع النطاق في جميع الصناعات فووفقاً لشركة جارتنر، من المتوقع أن يكون لدى 50% من المؤسسات سياسة لأمن المعلومات تعتمد على إطار عمل الأمن السيبراني NIST بحلول عام 2025، مما يسلط الضوء على الانتشار المتوقع لهذا الإطار التأسيسي لحوكمة الأمن السيبراني(Li et al,2019).

عاشرا: مراجعة الادبيات

في دراسة بعنوان " Measuring impact of cybersecurity on the performance of industrial control systems" هدفت الي دراسة تأثير الأمن السيبراني على أداء أنظمة التحكم الصناعية (ICS) وتسليط الضوء على أهمية أنظمة التحكم، المضمنة في مختلف الأنظمة الهندسية، بما في ذلك السيارات والمنازل والمكاتب والمنشآت الصناعية والبنى التحتية الحيوية مثل محطات الطاقة ومحطات معالجة المياه وأنظمة النقل وقد تم إنشاء قاعدة اختبار الأمن السيبراني NIST ICS، والتي كانت بمثابة بيئة عينة لتسهيل قياس أداء العمليات الصناعية للأنظمة المجهزة بتقنيات الأمن السيبراني واسفرت النتائج الي انه يوفر الاختبار رؤى قيمة حول تأثير تقنيات الأمن السيبراني على أداء أنظمة التحكم الصناعية، وبالتالي المساهمة في تحسين الأساليب والممارسات والمزالق عند تطبيق برنامج الأمن السيبراني على ICS. Stouffer et al (,2014)

وفي دراسة بعنوان" Cybersecurity in the internet of things in industrial management" هدفت الي دراسة تأثير الأمن السيبراني على أنظمة إنترنت الأشياء، لا سيما في سياق إنترنت الأشياء الصناعية (IIoT) وتسليط الضوء على المخاوف المتزايدة بشأن الأمن في مجالات المنازل الذكية والمدن الصناعية الذكية والرعاية الصحية، مع التركيز على مركزية الأمن لأنظمة إنترنت الأشياء لحماية البيانات الحساسة والبنية التحتية وقد تم مراجعة 70 مقالة رئيسية تم اكتشافها من خلال استطلاع عميق لأدبيات Scopus واسفرت النتائج الي تقديم رؤى حول المشهد المتطور للأمن السيبراني في سياق إنترنت الأشياء الصناعية، كما يتضح من مراجعة الأدبيات ذات الصلة (Raimundo et al,2022).

بينما في دراسة بعنوان" Digital transformation success under Industry 4.0: A strategic guideline for manufacturing SMEs" هدفت الي تزويد الشركات الصناعية الصغيرة والمتوسطة الحجم بمبادئ توجيهية لنجاح التحول الرقمي في ظل الصناعة 4.0 و تحديد محددات نجاح التحول الرقمي من خلال مراجعة الأدبيات التي تركز على المحتوى وتنفيذ النمذجة الهيكلية التفسيرية لاستخراج الترتيب الذي يجب أن تتواجد به محددات النجاح لتسهيل نجاح التحول الرقمي للشركات الصغيرة والمتوسطة على النحو الأمثل واسفرت النتائج الي ان أحد عشر من محددات النجاح الحيوية لجهود التحول الرقمي التي تبذلها الشركات الصغيرة والمتوسطة، ويكشف أن الدعم الخارجي للتحول الرقمي هو الخطوة الأولى في ضمان نجاح التحول الرقمي بين الشركات الصغيرة والمتوسطة، في حين تم تحديد الاستعداد التكنولوجي للعمليات باعتباره محدد النجاح الذي يتعذر الوصول إليه، وتسلط الدراسة الضوء على الأولوية الاستراتيجية لكل محدد بناء على قوته الدافعة وقوة الاعتماد عليه ويؤكد على أهمية فهم مفهوم التحول الرقمي في التصنيع في ظل الصناعة 4.0 وتطوير استراتيجيات قوية لتوجيه عملية التحول

الرقمي بشكل فعال للشركات المصنعة الصغيرة (Ghobakhloo et al,2021).

*** النتائج**

قد أسفرت الدراسة عن النتائج التالية:-

١- سلطت الدراسة الضوء على أهمية تحديد ثغرات أمنية محددة في سياق التحول الرقمي داخل المؤسسات الصناعية، من خلال دراسة نقاط الضعف السائدة مثل المخاطر الأمنية السحابية، والتحديات الأمنية لإنترنت الأشياء والتكنولوجيا التشغيلية، ونقاط الضعف في سلسلة التوريد، فقد قدمت الدراسة فهمًا شاملاً لمشهد التهديد الذي تواجهه المنظمات الصناعية.

٢- أكدت الدراسة على اعتماد أطر الأمن السيبراني الراسخة مثل NIST Cybersecurity Framework، ISO/IEC 27001، و CIS Critical Security Controls كمكونات أساسية لموقف الأمن السيبراني الاستباقي.

٣- بحث الدراسة في تأثير قوانين الأمن السيبراني، بما في ذلك اللائحة العامة لحماية البيانات (GDPR)، وقانون خصوصية المستهلك في كاليفورنيا (CCPA)، وقانون قابلية نقل التأمين الصحي والمساءلة (HIPAA)، على المؤسسات الصناعية لدراسة الآثار المالية والتشغيلية لعدم الامتثال التنظيمي وضرورة مواءمة ممارسات الأمن السيبراني مع المتطلبات القانونية.

٤- تناولت الدراسة الالتزام المالي الكبير بالاستعداد للأمن السيبراني في المؤسسات الصناعية، مع تسليط الضوء على الإنفاق المتوقع على المنتجات والخدمات المتعلقة بالأمن وشدد على العلاقة بين الاستثمار الاستباقي في الأمن السيبراني والاستعداد للاستجابة للحوادث في التخفيف من تأثير الثغرات الأمنية أثناء التحول الرقمي.

٥- أكدت الدراسة على الحاجة إلى تطوير إرشادات شاملة للأمن السيبراني مصممة خصيصًا لتلبية الاحتياجات المحددة للمؤسسات الصناعية التي تمر بالتحول الرقمي. وسلطت الضوء على محددات النجاح الرئيسية والأولويات الاستراتيجية الضرورية لتوجيه عملية التحول الرقمي بفعالية مع معالجة مشهد الأمن السيبراني المتطور.

*** التوصيات**

١- يجب على المؤسسات الصناعية إعطاء الأولوية لاعتماد أطر الأمن السيبراني الراسخة مثل NIST Cybersecurity Framework، ISO/IEC 27001، و CIS Critical Security Controls لتوفير نهج منظم لإدارة الأمن السيبراني في سياق التحول الرقمي حيث توفر هذه الأطر إرشادات شاملة لتحديد التهديدات السيبرانية وحمايتها وكشفها والاستجابة لها والتعافي منها، بما يتماشى مع الاحتياجات الديناميكية للعصر الرقمي.

٢- يعد تنفيذ تقييمات منتظمة لنقاط الضعف وممارسات إدارة المخاطر أمرًا ضروريًا لتحديد وتخفيف تهديدات الأمن السيبراني المتطورة فيجب على المؤسسات الصناعية الاستثمار في أدوات وعمليات قوية لإدارة الثغرات الأمنية لمعالجة الثغرات الأمنية بشكل استباقي وتحديد أولويات استراتيجيات تخفيف المخاطر لحماية الأصول والبيانات الهامة.

٣- نظرًا للمشهد التنظيمي المتنوع، يجب على المؤسسات الصناعية ضمان الامتثال للوائح الأمن السيبراني الخاصة

بالصناعة مثل اللائحة العامة لحماية البيانات (GDPR)، وقانون خصوصية المستهلك في كاليفورنيا (CCPA)، واللوائح الخاصة بقطاعات محددة. المعايير ويستلزم ذلك فهمًا شاملاً للمتطلبات القانونية وتنفيذ تدابير الأمن السيبراني المصممة خصيصًا للحفاظ على الالتزام التنظيمي.

٤- يعد تعزيز الوعي بالأمن السيبراني وبرامج التدريب بين الموظفين أمرًا ضروريًا لتنمية ثقافة تنظيمية مرنة عبر الإنترنت فيجب على المؤسسات الصناعية الاستثمار في مبادرات التعليم والتدريب المستمرة لتعزيز المعرفة بالأمن السيبراني لدى القوى العاملة لديها، وتمكين الموظفين من التعرف على التهديدات السيبرانية والاستجابة لها بشكل فعال.

٥- تعزيز التعاون بين المؤسسات الصناعية والهيئات الحكومية والمؤسسات البحثية وشركاء الصناعة لمشاركة أفضل الممارسات ومعلومات التهديدات ورؤى الأمن السيبراني فيمكن للمبادرات التعاونية مثل منصات تبادل المعلومات، واتحادات الصناعة، والشراكات بين القطاعين العام والخاص أن تعزز المرونة الجماعية للأمن السيبراني للنظم الإيكولوجية الصناعية وتساهم في الاستجابة الاستباقية للتهديدات السيبرانية الناشئة.

٦- احتضان التقنيات الناشئة مثل الذكاء الاصطناعي والتعلم الآلي والأتمتة لتعزيز قدرات الأمن السيبراني داخل المؤسسات الصناعية ويمكن لهذه التقنيات أن تعزز اكتشاف التهديدات والاستجابة للحوادث وتخفيف المخاطر، مما يتيح اتباع نهج استباقي وتكيفي للأمن السيبراني في سياق التحول الرقمي.

٧- تنفيذ آليات المراقبة المستمرة وإنشاء الاستعداد للاستجابة للحوادث للكشف بسرعة عن حوادث الأمن السيبراني والتخفيف منها والتعافي منها وينبغي للمؤسسات الصناعية إعطاء الأولوية لإنشاء خطط قوية للاستجابة للحوادث، بما في ذلك تمارين الطاولة، لضمان الاستجابة الفعالة والمرونة في مواجهة التهديدات السيبرانية.

٨- إنشاء هياكل حوكمة قوية للأمن السيبراني وأدوار قيادية داخل المؤسسات الصناعية لدفع مبادرات الأمن السيبراني وضمان التوافق التنظيمي مع أفضل ممارسات الأمن السيبراني ويستلزم ذلك تعيين قادة متخصصين في مجال الأمن السيبراني، وإنشاء لجان للأمن السيبراني، ودمج الأمن السيبراني في عمليات صنع القرار الاستراتيجي.

٩- إجراء اختبارات منتظمة للمرونة وتمارين التخطيط لاستمرارية الأعمال لتقييم مدى استعداد المؤسسات الصناعية لتحمل الاضطرابات السيبرانية وضمان استمرارية العمليات فتتيح هذه التمارين التحقق من صحة تدابير الأمن السيبراني وتحديد مجالات التحسين لتعزيز المرونة التنظيمية.

*** الخاتمة**

في الختام، سلطت الدراسة حول استراتيجيات تعزيز الأمن السيبراني في المؤسسات الصناعية في إطار التحول الرقمي الضوء على الضرورات الحاسمة اللازمة لتعزيز مرونة الأمن السيبراني في المشهد الديناميكي للرقمنة الصناعية. وتؤكد النتائج الطبيعة المتعددة الأوجه لتحديات الأمن السيبراني التي تواجهها المؤسسات الصناعية وتؤكد على التدابير الاستراتيجية الأساسية للتغلب على تعقيدات التحول الرقمي مع حماية البنية التحتية الحيوية والبيانات الحساسة.

فإن استكشاف الدراسة لنقاط الضعف في الأمن السيبراني، واعتماد الأطر الراسخة، والامتثال لقوانين الأمن السيبراني، والاستثمار في الاستعداد للأمن السيبراني، وتطوير مبادئ توجيهية مخصصة، وجهود التعاون قد وفر فهمًا شاملاً للاستراتيجيات الاستباقية المطلوبة لمعالجة مشهد الأمن السيبراني المتطور داخل البيئات الصناعية و تعتبر هذه الأفكار محورية في توجيه المؤسسات الصناعية نحو نهج شامل ومتكيف للأمن السيبراني في سياق التحول الرقمي.

ومع استمرار المؤسسات الصناعية في تبني التحول الرقمي، تدعو الدراسة إلى اتباع نهج استباقي وتعاوني للأمن السيبراني يدمج أفضل الممارسات والالتزام التنظيمي والاستثمار الاستراتيجي للتخفيف من التهديدات السيبرانية بشكل فعال، و تؤكد نتائج الدراسة على أهمية مواءمة مبادرات الأمن السيبراني مع الرحلة التحويلية للمؤسسات الصناعية، مما يضمن أن يكون الابتكار الرقمي مصحوبًا بتدابير قوية للأمن السيبراني تحمي الأصول الحيوية وتحافظ على استمرارية العمليات.

وتمتد الآثار المترتبة على هذا البحث إلى ما هو أبعد من الخطاب النظري، حيث تقدم إرشادات قابلة للتنفيذ للمؤسسات الصناعية التي تسعى إلى تعزيز وضع الأمن السيبراني لديها وسط نموذج التحول الرقمي، ومن خلال تبني الاستراتيجيات متعددة الأوجه الموضحة في هذه الدراسة، يمكن للمؤسسات الصناعية التغلب على تعقيدات التحول الرقمي بثقة ومرونة واتباع نهج استباقي للأمن السيبراني يتماشى مع المتطلبات الديناميكية للعصر الرقمي.

*** المراجع**

أولاً– المراجع العربية

عبدالناصر محمد أيوب، أحمد محمد البغدادي. (2022). الأخلاق والقانون والسن السيبراني. مجلة بنها للعلوم الإنسانية, 1(2), 1-25.

نورهان صبحي محمد عطية,. (2022). أثر تطبيق التحول الرقمي على تحسين الأداء الاستراتيجي للشركات الصناعية المقيدة بالبورصة المصرية. المجلة العلمية للدراسات والبحوث المالية والإدارية ,(2)13 , 500-524.

عمار ياسر البابلي، (2021). نظرة عامة على تأثير الخطأ البشري على الأمن السيبراني بناءً على ISO/IEC 27001 لإدارة أمن المعلومات. مجلة أبحاث أمن المعلومات والجرائم الإلكترونية, 4(1), 95-102.

احمد مجر، صفاء غنيم. (2022). تطوير أداة لقياس كفاءة التحول الرقمي للمدن العربية نحو المدن الذكية بالتطبيق على حالتين دراسيتين: مدينة ينبع البحرو مدينة ينبع الصناعية بالمملكة العربية السعودية. المجلة الدولية للتنمية, 11(1), 61-82.

ثاقب سعيد ، صالحة عبد التميمي ، نورة الكيال ، ابتسام الشهري ، دينا عبد العباد، تحديات التحول الرقمي والأمن السيبراني أمام مرونة الشركات: القضايا والتوصيات. مجسات (بازل). 2023

بوحنية قوي. (2023). التعليم العالي في الجزائر في ظل الثورة الصناعية الرابعة-الإجراءات القانونية والتنظيمية ومؤشرات التكيف مع التحول الرقمي. مجلة جامعة فزان التطبيقية, 25-39.

ماجده عبد الشافى محمد الهادى خالد. (2023). الحماية الدستورية للأمن السيبرانى وأثره على النظام العام. مجلة البحوث القانونية والاقتصادية-المنوفية, 57(4), 345-410.

ناصر بن محمد بن عباس. (2020). تدابير وقائية مقترحة للوقاية من الجرائم السيبرانية: دراسة ميدانية (Doctoral dissertation, جامعة نايف العربية للعلوم الأمنية)،ص23-112

وفاء لطفى, (2022). الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني: التجربة الماليزية نموذجا. مجلة كلية الاقتصاد والعلوم السياسية, 23(1), 151-178.

محمد حسن عماد مكاوي, . (2022). الخصوصية الرقمية في القانون الدولي والمواثيق الدولية. مجلة البحوث والدراسات الإعلامية, 20(20), 1-74.

هبة جمال الدين, (2023). الأمن السيبراني والتحول في النظام الدولي. مجلة كلية الاقتصاد والعلوم السياسية, 24(1), 189-230.

لمياء زواوي, فهيم رملي. (2023). كتاب السيبرانية وأمن المجتمع الرقمي: دراسة حالة الجزائر. المجلة الجزائرية للأمن والتنمية, 12(02), 148-160.

ثانياً- المراجع الاجنبية

Stouffer, K., Candell, R. (2014). Measuring impact of cybersecurity on the performance of industrial control systems. Mechanical Engineering, 136(12), S4-S7.

Raimundo, R. J., & Rosário, A. T. (2022). Cybersecurity in the internet of things in industrial management. Applied Sciences, 12(3), 1598.

Ghobakhloo, M., & Iranmanesh, M. (2021). Digital transformation success under Industry 4.0: A strategic guideline for manufacturing SMEs. Journal of Manufacturing Technology Management, 32(8), 1533-1556.

Ncubukezi, T. (2022, March). Human errors: A cybersecurity concern and the weakest link to small businesses. In Proceedings of the 17th International Conference on Information Warfare and Security (p. 395.(

Cheng ECK, Wang T. Institutional Strategies for Cybersecurity in Higher Education Institutions. Information. 2022; 13(4):192

management system standard ISO/IEC 27001: a web mining-based analysis. IEEE Transactions on Engineering Management, 68(1), 87-100.

Li, H., Yu, L., & He, W. (2019). The impact of GDPR on global technology development. Journal of Global Information Technology Management, 22(1), 1-6 .

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. Sensors, 23(15), 6666.

Comizio, V. G., Dayanim, B., & Bain, L. (2016). Cybersecurity as a global concern in need of global solutions: an overview of financial regulatory developments in 2015. Journal of Investment Compliance, 17(1), 101-111.

Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). Analysis of cybersecurity standard and framework components. International Journal of Communication Networks and Information Security, 12(3), 417-432.

He, W., & Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. Journal of Organizational Computing and Electronic Commerce, 29(4), 249-257.

Mirtsch, M., Kinne, J., & Blind, K. (2020). Exploring the adoption of the international information security