هما مجالان أساسيان في عالم التكنولوجيا الحديثة ومفصليان لضمان حماية وسرية المعلومات في العصر الرقمي الذي نعيش فيه. يشير أمن المعلومات إلى مجموعة من الإجراءات والسياسات والتقنيات المصممة لحماية سرية المعلومات وسلامتها وضمان توفرها، وذلك من خلال مواجهة التهديدات والمخاطر المحتملة مثل الوصول غير المصرح به، إدارة المخاطر من جانبها تُعنى بكافة الخطوات والعمليات اللازمة لتحديد وتقييم ومعالجة ومراقبة وتقليل التأثيرات السلبية للمخاطر الأمنية المحتملة. تُعتبر هذه الإدارة جزءًا حيويًا لأنها تساهم في تمكين المؤسسات من استيعاب التهديدات بشكل أفضل والحد منها عبر اتخاذ قرارات مدروسة تقلل الخسائر المتوقعة. ولا تقتصر إدارة المخاطر على الجوانب التقنية فقط، إضافة إلى تعزيز ثقافة تُقدّر أهمية التعامل المنظم والفعال مع المخاطر. بفضل الاستراتيجيات الفعالة لإدارة المخاطر، تتزايد أهمية أمن المعلومات وإدارة المخاطر سواء على مستوى الشركات أو الأفراد. هذا التكامل بين المجالين يُعد ضرورة لضمان استمرارية الأعمال وحماية البيانات والمعلومات الحساسة ضمن السياق الرقمي المتسارع. و عملية إدارة المخاطر المرتبطة باستخدام تكنولوجيا المعلومات. وهي تتضمن تحديد وتقييم ومعالجة المخاطر التي تهدد سرية المعلومات في أصول المنظمة. والهدف النهائي من هذه العملية هو معالجة المخاطر وفقًا لتحمل المنظمة للمخاطر بشكل عام. لا ينبغي للشركات أن تتوقع القضاء على جميع المخاطر؛ بل يجب عليها بدلاً من ذلك أن تسعى إلى تحديد مستوى المخاطر المقبول لمؤسستها وتحقيقه. وتوفر للمؤسسات إطارًا منظمًا للكشف عن المخاطر المحتملة على أصولها القيمة وتقييمها والتخفيف منها. مشكلة أمن المعلومات وإدارة المخاطر تمثل تحديات كبيرة تعترض طريق المؤسسات والأفراد في عصر التكنولوجيا الحديثة، 2. ضعف التوعية الأمنية بين الموظفين والأفراد يُعتبر عاملاً يزيد احتمالية التعرض للاختراقات والهجمات نتيجة لعدم اتباع ممارسات السلامة الرقمية. تبرز تحديات جديدة ترتبط بالاعتماد على التشفير الكمي وضمان الحماية الآمنة للأنظمة المتصلة. كشركة طيران تعمل بشكل يومي في مطارات هناك بعض مشاكل المعينة التي تواجه الشركة كنظام تقني في المنظومات الخاصة بها. منها منظومة قبول ركاب أو خدمات الركاب حيث تعمل بنظام و المشكلة التي تواجه هذه منظومة هي آلية الربط بين (أماديوس) و أجهزة (Customer management) (أماديوس) كمنظومة هو (VPN: Virtual Private Network) خاص بعملية ربط لتشغيل منظومات خاصة بهم. و (VPN) خاصة بها فيتم استخدام شبكة خاصة افتراضية، و لتشغيل هذه أنظمة يجب توفير شركة خاصة تقوم بهذه عملية كمزود خدمة لشركة خطوط ليبية في متواجد في طرابلس فأي ضعف في شبكة أنترنت يسبب في تعطيل رحلات المتواجدة لدينا. و يمكن أن يسبب (VPN) بنغازي، و مشاكل لنظام الشركة عن طريق فتح رابط أو استخدام مواقع أو غيرها. تتمثل مشكلة الدراسة في عدم وجود إدارة للمخاطر وأمن في المطارات الدولية ذات كفاءة وفاعلية في مواجهة المخاطر التي تؤدي إلى خسائر مادية حيث يتولد عن قبول المخاطر في المطارات خسائر كبيرة مما يتطلب وجود نظام وبرامج لإدارة هذه المخاطر والسيطرة عليها وان عدم وجود إدارة للمخاطر قد يزيد من احتمالات تحقيق المخاطر في المطارات الدولية. 1.3. 1.حماية السرية و الخصوصية ضمان عدم وصول أي شخص غير مخول إلى المعلومات الحساسة أو الخاصة بشركة أو معلومات الافراد و بيانات الشخصية، و يستخدم جدار الحماية يدخل من خارج على أي موقع و يتحكم (IP) لحماية بيانات شركة، و من أهم مزايا جدار الحماية هو السيطرة على أي (Firewall) في تتبع معلومات و أي ثغره موجوده يغلقها و يستطيع معرفة أي جهاز يوجد بيه مشكلة، 2. توفير و مراقبة الوصول وتثقيف و التوعية ضمان توفر النظم والمعلومات في الأوقات المطلوبة دون تعطيلات غير مبرمجة أو هجمات و مراقبة منح الوصول فقط للأشخاص المصرح لهم، تعزيز الوعي بأمن المعلومات وتعليم المستخدمين كيفية التصرف بأمان في استخدام التقنيات الحالية و الجديدة لأن جدار الحماية يوجد له أنواع متعددة و يجب من الخبرة لتعامل معه لحماية نظام الشركة و هذا الهدف من الدراسة خاص لمدينة بنغازي لضمان عدم حصول عطل أو (VPN) تجنب أي مشكلة في الشركة و تسارع في حلها. 3. و يجب توفير تأخير في رحلات الركاب، و عمل دورات توعية لهم و توظيف موظفين ذو خبرة من كلية تقنية المعلومات لإعطاء طابق تقني جديد للشركة. 4. كلا من أمن المعلومات وإدارة المخاطر يساهمان في تعزيز استدامة ونجاح المؤسسات والأفراد، من خلال حماية البيانات الحساسة، وتحقيق مزيد من الشفافية والمساءلة. 2. يستعرض أهمية تعزيز أمن المعلومات داخل الشركة والتخلي عن الطرق التقليدية المستخدمة في حماية البيانات. وتقييم البرامج وأنواع الأجهزة المستخدمة ضمن الشبكة، بالإضافة إلى استعراض آراء الموظفين بشأن هذه العمليات. 1.5. كما قام الباحث بعمل الاتي قمنا بإنشاء دراسة كاملة عن أمن معلومات الشركة و كيفية التعامل مع المخاطر و إدارتها و معرفة اراء الموظفين و المُدراء في إدارة، بالإضافة إلى ابحث عن دراسات سابقة في توزيع و حساب نتائج الاستبيان (Excel Microsoft) حديثة تتحدث عن عنوان البحث. الجانب العلمي تم استخدام برنامج

احصائيا و تم حساب كلا من (المتوسط الحسابي/ الانحراف المعياري/ النسبة المئوية/ اتجاه العينة)، و تم شرح كل سؤال و عمل جدول خاص لكل سؤال لتوضيح النسب المئوية و من ثم عمل جدول و شرح اتجاه العينة و تمت مناقشة و شرح الأسئلة بصفة عامة. 1.6 . 1.6 . و يتضمن أمن المعلومات تطبيق تقنيات وأساليب مثل التشفير، والتحقق من الهوية، وتقييم تأثيرها، 3.2. يتطلب دمج المعرفة التقنية والإدارية مع استراتيجيات واضحة مثل تطوير استراتيجيات قائمة على البيانات جمع وتحليل البيانات و التحليل الإحصائي، و الاستفادة من الخبرات والأبحاث أي الاستفادة والاستعانة بخبراء أمان المعلومات وإدارة المخاطر للحصول على رؤى متعمقة وتوجيهات و مراجعة الأبحاث الاطلاع على أحدث الأبحاث والتطورات في مجال الأمن وإدارة المخاطر، و تحسين التواصل مع إدارات العليا و الموظفين و فريق لعمل في حالة العمل على مشروع. و تطبيق منهجيات اتخاذ القرارات مثل تحليل تكلفة فائدة، والتحليل الاستراتيجي لـتطبيق التحليل الاستراتيجي لتقييم الخيارات المختلفة وتحديد الخيار الأنسب بناءً على الأهداف والمخاطر. و كما يجب توفير التدريب والتطوير المستمر أي تقديم التدريب المستمر للموظفين على أحدث الممارسات والتقنيات في مجال الأمان وإدارة المخاطر، و تحديث المهارات لـتشجيع التعلم المستمر وتحديث المهارات لمواكبة التغيرات في التهديدات والتقنيات. مما يؤدي إلى حماية أفضل للأصول وتقليل المخاطر بشكل أكثر فعالية. 3.3. هو مهندس من كلية تقنية المعلومات من قسم الشبكات و اتصالات الحاسوب ليكون على درايه كافية بكافة المعلومات و يكون هناك خبير لإستخدام البرمجة و يجب توفير موظفين ذو خبرة من كافة الأقسام لتعامل مع جميع المشاكل التي قد تحدث مستقبلياً. 3.4. 3.4. والتي تشكل بدورها أساس البنية الأساسية الأمنية للمؤسسة. تعمل تلك العناصر الثلاثة بمثابة مبادئ توجيهية لتنفيذ خطة أمان المعلومات. يمثل تشفير البيانات والمصادقة متعددة العوامل وتفادي فقدان البيانات جزءاً من الأدوات التي يمكن للمؤسسات استخدامها للمساعدة في ضمان سرية البيانات. 3.4. ستدرك الشركات التي تتمتع بميزة أمان المعلومات الفعالة أهمية البيانات الدقيقة والموثوقة، ولن تسمح لأي مستخدم غير مُخوَّل بالوصول إليها أو تغييرها أو التدخل فيها بأي طريقة أخرى. تساعد أدوات مثل أذونات الوصول إلى الملفات وإدارة الهوية وعناصر التحكم في وصول المستخدم في ضمان تكامل البيانات. 3.4. صورة رقم 1. 3.4. وتقيّم مدى احتمالية وتأثير كل خطر. 3.4. 3.4. تقييم المخاطر، يجب إتمام كل مرحلة قبل الانتقال إلى المرحلة التالية. تلعب كل من هذه الخطوات دورًا حيويًا في صياغة استراتيجية شاملة لحماية المعلومات من خروقات الأمن المحتملة واختراق البيانات. الخطوة 1. بما في ذلك الأجهزة والأنظمة والتطبيقات والبيانات. بعد ذلك، مثل جدران الحماية ومراجعة السجلات. يتضمن ذلك رسم خرائط وتصنيف التهديدات والثغرات الأمنية بناءً على احتمالية حدوثها وتأثيرها. الخطوة 3. ومن المثالي أن تشمل خطة معالجة المخاطر العناصر التالية ـ التخفيف يركز على تقليل احتمالية حدوث المخاطر أو تأثيرها. ـ النقل يتم هنا نقل المخاطر إلى جهة أخرى، مثل شراء التأمين السيبراني، ـ القبول يتيح للمؤسسات اتخاذ قرار مدروس بقبول المخاطر، وهو مناسب للمخاطر ذات التأثير أو الاحتمالية المنخفضة، أو تلك التي تكون تكلفتها مرتفعة ويصعب تخفيفها. الخطوة 4. فإنه من الضروري مراقبة المخاطر المحددة والانتباه إلى الثغرات والتهديدات الجديدة. ولذات السبب، 3.6. إدارة مخاطر تكنولوجيا المعلومات هي عملية إدارة المخاطر والتخفيف من حدتها من خلال التخطيط الدقيق والأنظمة المتخصصة والمبادئ التوجيهية والسياسات والقرارات عبر مختلف القطاعات ، وليس الأمن السيبراني فقط. يركز طاقم تكنولوجيا المعلومات بشكل كامل على التخفيف من مخاطر تكنولوجيا المعلومات. من ناحية أخرى ، كلا المصطلحين، عبارة عن كلمات طنانة غالبًا ما يتم طرحها في نفس السياق. ولا ينبغي استخدامهما بالتبادل. الأمن السيبراني هو مجموعة فرعية من أمن المعلومات، تشمل إدارة مخاطر أكثر بكثير من مجرد الجوانب الرقمية والفضائية الإلكترونية لحماية بيانات المؤسسة. وهو يشمل ويغطي أنواعًا أخرى من المخاطر، مثل عيوب الأجهزة والبرامج، والخطأ البشري، ومع ذلك، وهو الجانب الرئيسي لإدارة مخاطر. 3.7. لا تقتصر فوائد إدارة مخاطر أمن المعلومات على الحماية من التهديدات الإلكترونية فحسب، بل تسهم أيضًا في تعزيز ثقافة الوعي والمساءلة داخل مؤسستك. يمكن لاستراتيجية فعالة في إدارة مخاطر أمن المعلومات أن تلعب دورًا حيويًا في نجاح عملك واستمراريته. بدءًا من حماية المعلومات الحساسة للعملاء وصولاً إلى ضمان استمرارية الأعمال، تشمل الفوائد جوانب متعددة من عملياتك. 3.7. يلعب التشفير دورًا أساسيًا في هذه الاستراتيجية، مما يقلل من التهديدات الداخلية والخارجية. تضمن الحماية الاستباقية للبيانات الكشف الفوري والاستجابة السريعة للحوادث الأمنية، مما يعزز الثقة بين جميع الأطراف المعنية. من خلال تنفيذ عملية إدارة بشكل فعال، يمكن لشركتك الامتثال لمتطلبات الصناعة وتفادي أي عواقب قانونية. مما (ISRM) المخاطر المتعلقة بالمعلومات يتيح الاستجابة السريعة للحوادث الأمنية. مما يجعل الموظفين أكثر استعدادًا للمشاركة في جهود التخفيف من التهديدات. 3.7.

يمكن لشركتك تجنب التكاليف المالية المرتبطة بالحوادث الأمنية وانتهاكات البيانات. مما يساعد في تقليل النفقات المتعلقة بالاستجابة للحوادث، بالإضافة إلى العواقب القانونية والأضرار التي قد تلحق بالسمعة. 3.7. بل تشمل أيضًا التعامل مع التهديدات المحتملة بشكل استباقي، مما يساهم في بناء أساس قوي من الثقة مع العملاء والشركاء وأصحاب المصلحة. في النهاية، هناك العديد من الأطر والأساليب لهذا، ولكنك ستستخدم على الأرجح بعض الاختلافات في هذه المعادلة المخاطر= (التهديد × الثغرة الأمنية (احتمالية الاستغلال × تأثير الاستغلال) × قيمة الأصول) ـ ضوابط الأمان. وهو ما يثير استياء الجميع. حيث عبّر معظم المشاركين عن رضاهم بشأن وجود هذه السياسات ومدى وضوحها. غياب التحديث الدوري يشكل خطرًا حقيقيًا في ظل التطورات السريعة في أساليب الهجمات الإلكترونية. علاوة على ذلك، خاصة فيما يتعلق بالتدريب الدوري على التهديدات الأمنية مثل التصيد الاحتيالي. أظهرت النتائج أن نسبة كبيرة من الموظفين لا يدركون أهمية تغيير كلمات المرور بانتظام أو الإبلاغ الفوري عن الحوادث الأمنية. هذه النتائج تشير إلى ضرورة تعزيز الثقافة الأمنية داخل المؤسسة من خلال برامج تدريب متقدمة وشاملة. حيث يشكل الذكور النسبة الأكبر من الموظفين مقارنة بالإناث. كما تبين أن نسبة حملة الدكتوراه منخفضة جدًا، مما يعكس نقصًا في استقطاب الكفاءات الأكاديمية ذات الخبرة العالية. هذه الفجوة قد تؤثر على قدرة الشركة على مواجهة التحديات الأمنية بأسلوب أكثر استراتيجية وابتكارًا. 4. مستوى الاعتماد على التقنيات الأمنية توضح النتائج أن الشركة تعتمد على تقنيات إلا أن هناك مؤشرات على وجود نقاط ضعف في هذه الأدوات. يشكلان ،(VPNمثل برامج مكافحة الفيروسات وشبكات (الـ تحديات حقيقية تعيق أداء الشركة. مما يشير إلى الحاجة لتحديث هذه البرامج باستمرار وضمان كفاءتها. 5. تقييم المخاطر وإدارة الحوادث الأمنية بيّنت النتائج أن الشركة تواجه تحديات في تقييم المخاطر الأمنية بشكل منتظم. المشاركون أشاروا إلى أن الشركة تحتاج إلى تحسين آليات اكتشاف الثغرات ومعالجتها، إضافة إلى ضرورة وجود خطط واضحة لإدارة الحوادث الأمنية. 6. رضا الموظفين عن السياسات الأمنية على الرغم من وجود رضا عام عن السياسات الأمنية، الخلاصة مع التركيز على شركة الخطوط الجوية الليبية كمثال عملي لدراسة تطبيقات هذه المبادئ في قطاع حساس ومهم. تم استعراض الجوانب النظرية لإدارة المخاطر وأمن المعلومات، إلى جانب تحليل البيانات العملية المستخلصة من استبيان استهدف تقييم الوضع الحالي للشركة فيما يتعلق بتلك القضايا. ويمكن تلخيص النتائج الرئيسية في النقاط التالية ومع ذلك، مثل تحديثها بشكل دوري أو تدريب الموظفين عليها، أشار العديد من المشاركين إلى أن تلك السياسات تُطبّق بفعالية، ضعف الوعي الأمني لدى بعض الموظفين، هذا الضعف يمثل خطرًا كبيرًا، 3. التنوع الوظيفي أظهرت البيانات فجوة كبيرة في التوزيع النوعي للقوى العاملة، حيث تمثل النساء نسبة صغيرة جدًا من العاملين مقارنة بالذكور. بالإضافة إلى ذلك، هناك نقص واضح في الكوادر الأكاديمية ذات الخبرة العالية (حملة الدكتوراه)، مما قد يؤثر سلبًا على قدرة الشركة على تطوير استراتيجيات متقدمة لإدارة المخاطر وأمن المعلومات. 4. التقنيات لحماية البيانات وربط المواقع البعيدة، ولكن تم الإبلاغ عن تحديات (VPN المستخدمة الشركة تعتمد على تقنيات مثل شبكات (الـ متعلقة بضعف الإنترنت وتأثيره على كفاءة الأنظمة. كما أن بعض المشاركين أعربوا عن قلقهم بشأن عدم وجود آليات فعالة للتعامل مع الأجهزة القديمة وضمان حذف البيانات منها بشكل آمن. 5. تخصيص الموارد أظهرت النتائج أن هناك نقصًا في تخصيص ميزانيات كافية لتحسين أدوات وتقنيات إدارة المخاطر. هذا النقص ينعكس سلبًا على قدرة الشركة على مواجهة التهديدات الأمنية المتزايدة، خاصة مع تطور التكنولوجيا وزيادة التعقيد في الهجمات السيبرانية. 5.2. 1. الفجوة بين النظرية والتطبيق على الرغم من وجود سياسات أمنية واضحة، إلا أن التنفيذ العملي لها يواجه تحديات مرتبطة بضعف الموارد والتدريب. 2. التأثير البشري يظهر البحث أن العامل البشري يظل أحد أهم الجوانب التي تحتاج إلى تحسين في الشركة. ضعف الوعي الأمني لدى الموظفين يجعلهم هدفًا سهلًا للهجمات الإلكترونية، مما يستدعي استراتيجيات شاملة للتدريب والتوعية. أي تأخير في تحديث الأنظمة أو تخصيص موارد إضافية قد يزيد من احتمالية وقوع حوادث أمنية. خاصة تلك التي تعمل في قطاعات حيوية مثل الطيران. 2. تخصيص ميزانيات ملائمة لأمن المعلومات وإدارة المخاطر يمثل استثمارًا استراتيجيًا طويل الأمد. 3. التطوير المستمر للأنظمة والتقنيات ضروري لمواجهة التحديات الأمنية المتزايدة. 5.4. 3. تعزيز التنوع في الهيكل الوظيفي من خلال ،استقطاب الكوادر الأكاديمية والخبرات النسائية. 4. اعتماد آليات دورية لتقييم المخاطر الأمنية واختبار الأنظمة. في الختام