ثقافة الأمن الإلكتروني في مجال الطيران المدني

نشرت بموجب سلطة الأمين العام

يناير ٢٠٢٢

منظمة الطيران المدني الدولي

١- المُقدِّمة

تتماشى هذه الإرشادات مع استراتيجية الإيكاو للأمن الإلكتروني في مجال الطيران[١] وخطة عمل الأمن الإلكتروني[٢]، التي يوصي بندها الإجرائي CyAP7.1 بتعريف ثقافة الأمن الإلكتروني في مجال الطيران المدني والتوعية بشأنها والترويج لها.

٢- النطاق

الهدف من هذه الإرشادات هو دعم الدول الأعضاء وأصحاب المصلحة من أجل تصميم وتنفيذ ثقافة الأمن الإلكتروني وترسيخها داخل منظماتهم. والهدف النهائي هو دعم الأمن الإلكتروني للطيران المدني وتعزيز قدرته على الصمود في مواجهة التهديدات والمخاطر الإلكترونية.

٣- تعريف ثقافة الأمن الإلكتروني وتحديد أهدافها العامة ومنافعها

٣-١ لأغراض هذه الإرشادات، من المفهوم عموماً أن ثقافة الأمن الإلكتروني تشير إلى مجموعة من الافتراضات والمواقف والمعتقدات وأنماط السلوك والمعايير والتصوُّرات والقيم المتأصلة في العمليات اليومية للمنظمة، وتنعكس في تصرفات وأنماط سلوك جميع الكيانات والموظفين في تفاعلهم مع الأصول الرقمية.

٣-٢ تهدف ثقافة الأمن الإلكتروني الإيجابية إلى جعل اعتبارات الأمن الإلكتروني جزءًا من عادات المنظمة وعملياتها وتصريف أمورها وسلوكها، وذلك من خلال تضمينها في العمليات اليومية بحيث تنعكس في تصرفات جميع الموظفين وأنماط سلوكهم.

٣-٣ يساعد إنشاء ثقافة راسخة وفعَّالة للأمن الإلكتروني، كجزء لا يتجزأ من الثقافة التنظيمية، المنظمات على تحسين أدائها العام من خلال التحديد المبكر للمخاطر الإلكترونية المحتملة.

٣-٤ تعتمد ثقافة الأمن الإلكتروني في مجال الطيران المدني على خبرة القطاع وجهوده ومدى نجاحه في إرساء ثقافة السلامة والثقافة الأمنية في مجال الطيران، وتبادل العديد من العناصر الأساسية فيما بين الثلاث ثقافات. ولا تؤدي هذه الطبيعة الشاملة لثقافة الأمن الإلكتروني على نطاق القطاع إلى تعزيز وضع الأمن الإلكتروني فحسب، بل تؤدي أيضاً إلى امتداد إيجابي عبر الثلاث ثقافات يدعمها جميعاً ويعززها ويرسخ مكانتها.

٣-٥ يمكن القول بإيجاز، بأن ثقافة الأمن الإلكتروني تسمح لكل شخص في المنظمة، بغض النظر عن دوره، بتحسين أدائه في البيئة الرقمية. ومن الأمثلة على فوائد تصميم وتنفيذ ثقافة الأمن الإلكتروني الفعَّالة الراسخة ما يلي:

أ) تعزيز نضج المنظمة في مجال الأمن الإلكتروني؛
ب) تعامل جميع الموظفين مع المعلومات بالشكل المناسب؛
ج) تحسين وضع الأمن الإلكتروني بما يدعم فعالية المنظمة وكفاءتها في ما يتعلَّق بالتخفيف من المخاطر الإلكترونية؛
د) إذكاء وعي جميع الموظفين بالمخاطر الإلكترونية، وما يتعيَّن عليهم القيام به بشكل فردي في تحديد تلك المخاطر والتخفيف من حدتها؛
هـ) الاستعداد للإفادة بشأن الرقابة الشخصية في تطبيق العمليات والإجراءات التنظيمية للأمن الإلكتروني فضلاً عن الإبلاغ عن الأنشطة الإلكترونية المشبوهة، مما يؤدي إلى استباقية الكشف بشكل أفضل عن المخاطر الإلكترونية.

---

[١] https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx

[٢] كتاب المنظمة SL 2020/114

٣-٥ ترد في الأقسام التالية من هذه الإرشادات العناصر الأساسية لثقافة الأمن الإلكتروني التنظيمية الفعَّالة في مجال الطيران. ومع ذلك، فعلى الرغم من تعريف هذه العناصر الأساسية بشكل جيد، إلا أنه يجب تصميم ثقافة الأمن الإلكتروني بشكل منفرد داخل كل منظمة. وينبغي أخذ كافة الجوانب المختلفة في الاعتبار، بما في ذلك مستوى النضج التنظيمي في ما يتعلَّق بالأمن الإلكتروني، والثقافات والقيم القائمة، والمشهد العام للتهديدات في مجال الأمن الإلكتروني.

٣-٧ فيما يلي العناصر الأساسية لثقافة الأمن الإلكتروني الراسخة الفعَّالة في مجال الطيران المدني:

أ) القيادة؛
ب) الروابط بين كافة المجالات؛
ج) الإعلام والاتصال؛
د) إذكاء الوعي والتدريب والتعليم؛
هـ) نُظُم الإبلاغ؛
و) الاستعراض والتحسين بشكل مستمر؛
ز) وجود بيئة عمل إيجابية.

٤- القيادة

٤-١ تعتمد ثقافة الأمن الإلكتروني الفعَّالة على مدى التزام كل شخص في المنظمة، بدءًا بالإدارة العليا التي ينبغي لها إبداء الالتزام الكامل بثقافة الأمن الإلكتروني، في جميع الأوقات وعلى نطاق جميع الأنشطة والاستراتيجيات والسياسات والأهداف التنظيمية.

٤-٢ ينبغي للإدارة العليا الامتثال لسياسات الأمن الإلكتروني، وأن تكون قدوة يحتذي بها مديرو المنظمة وموظفوها. كما ينبغي لها أن تدعو إلى الأمن الإلكتروني باعتباره قيمة مؤسسية فضلاً عن كونه قيمة شخصية، بينما تعمل بالمثل على مواءمة سلوكها مع هذه القيمة.

٤-٣ وفي هذا الصدد، ينبغي للإدارة العليا أن:

أ) تسعى إلى تعزيز معرفتها بالأمن الإلكتروني في مجال الطيران المدني؛
ب) تلتزم بقواعد الأمن الإلكتروني وعملياته وإجراءاته في جميع الأوقات، وأن تكون قدوة للمنظمة؛
ج) تدرج الأمن الإلكتروني بشكل واضح كأولوية تنظيمية؛
د) تكريس الأمن الإلكتروني في مجال الطيران في السياسات العامة المكتوبة للمنظمة كجزء جوهري من خطة إدارة الشركة؛
هـ) تقديم الدعم الواضح من أجل تنفيذ ثقافة الأمن الإلكتروني؛
و) ضمان ودعم التدريب على الأمن الإلكتروني وبناء القدرات من أجل جميع الموظفين؛
ز) ضمان تجهيز تقارير الأمن الإلكتروني في الوقت المناسب، وكذلك ضمان التنفيذ الفوري لأي إجراءات تصحيحية ووقائية مطلوبة؛
ح) التدخل بشكل مناسب كلما تعرَّض الأمن الإلكتروني للخطر؛
ط) رصد تطوُّر وضع الأمن الإلكتروني للمنظمة، وثقافة الأمن الإلكتروني، والتدابير والموارد المُخصَّصة لدعم التحسين المستمر في ما يتعلَّق بتبنّي ثقافة الأمن الإلكتروني على نطاق المنظمة.

٤-٤ وعلى خطى الإدارة العليا، ينبغي أيضاً للمستويات الإدارية المختلفة داخل المنظمة أن تسعى إلى تبنّي الإجراءات الواردة في الفقرة ٤-٣ أعلاه، بما يتماشى مع مسؤولياتها ونطاق إدارتها، وذلك من أجل نشر الالتزام بثقافة الأمن الإلكتروني على نطاق المنظمة.

٥- الروابط بين كافة المجالات

٥-١ مع مراعاة تعدد المخاطر الإلكترونية ونقاط الضعف الإلكترونية في كل منظمة، ينبغي رسمياً تحديد الروابط بين كافة المجالات.

٥-٢ يمكن تشكيل فرقة عمل متعددة التخصصات ترفع تقاريرها إلى الإدارة العليا كوسيلة لدعم تنسيق ثقافة الأمن الإلكتروني على نطاق المنظمة.

٥-٣ يتعين أن تشمل أهداف فرقة العمل هذه ما يلي:

أ) إجراء تقييم دوري لمستوى نضج ثقافة الأمن الإلكتروني داخل المنظمة؛
ب) تحديد المخاطر والفرص في ما يتعلق بتنفيذ ثقافة الأمن الإلكتروني؛
ج) التقريب بين وجهات نظر مختلف الأطراف المعنية داخل المنظمة في ما يتعلق بثقافة الأمن الإلكتروني؛
د) دعم تطوير وتنفيذ الأنشطة على نطاق كافة المجالات في ما يتعلَّق بتعزيز ثقافة الأمن الإلكتروني في المنظمة.

٦- الإعلام والاتصال

٦-١ للإعلام والاتصال دورٌ أساسيٌ، داخل المنظمة وخارجها، من أجل ضمان نجاح تنفيذ ثقافة الأمن الإلكتروني. وهما الوسيلة الرئيسية التي يمكن من خلالها بلوغ مستوى الوعي المنشود.

٦-٢ من أجل فعالية الإعلام والاتصال، ينبغي اعتبار المهارات التالية جزءًا من ثقافة الأمن الإلكتروني الراسخة:

أ) *الإنصات الفعَّال* – العملية التي يجري من خلالها ملاحظة الإشارات اللفظية وغير اللفظية، من أجل إعادة التعرف على قيم الغير واحتياجاتهم، والإسهام في تحسين التواصل بين أعضاء الفريق؛
ب) *تكييف أسلوب الإعلام والاتصال لمختلف الجماهير والأوضاع* – وفهم كيفية التواصل مع الغير وإعداد الرسالة بشكل مخصَّص من أجل التواصل معهم بشكل أفضل؛
ج) *وضوح الإعلام والاتصال* – تحديد ما الذي ينبغي الإعلام به وكيفية الإعلام به.

٦-٣ ينبغي للإدارة العليا أن تكفل إبلاغ جميع الموظفين على النحو الواجب بالسياسات والإرشادات الداخلية المُتعلِّقة بالأمن الإلكتروني، فضلاً عن مبررات وضعها والعمل بها. إذ إن برنامج التواصل الداخلي القوي يُسهم في قبول جميع الموظفين لتدابير الأمن الإلكتروني وفهمهم لها، كما يساعد على تعزيز ثقافة الأمن الإلكتروني في المنظمة.

٦-٤ وبالإضافة إلى ذلك، سيساعد برامج التواصل الداخلي إلى حد كبير على تحقيق ما يلي:

أ) التأكد من أن جميع الموظفين على دراية تامة بواجباتهم وحقوقهم وآليات الإبلاغ المُطبَّقة في المنظمة؛
ب) تعزيز مدونة السلوك الرقمي التنظيمية، التي تشمل العمليات والتدابير والضوابط التي يجب على الموظفين الالتزام بها دائماً.

٧- إذكاء الوعي والتدريب والتعليم

٧-١ يمثل إذكاء الوعي والتدريب والتعليم مجالات رئيسية في عملية التعلُّم واستخلاص الدروس التي ينبغي الاستفادة منها من أجل بناء ثقافة أمن إلكتروني قوية. فالتوعية توفر المعرفة للناس، والتدريب يكسبهم المهارات، والتعليم يوفر المعرفة والمهارات ضمن إطار نظري، فيدمج بالتالي التوعية بالتدريب.

٧-٢ يجب على جميع موظفي الطيران المدني الذين يتعاملون مع الأصول الرقمية للمنظمة، بغض النظر عن أدوارهم أو وظائفهم، الخضوع لبرنامج للتوعية والتدريب والتعليم في مجال الأمن الإلكتروني من أجل ضمان تزويدهم بالمعرفة والمهارات اللازمين

بشأن مخاطر الأمن الإلكتروني في مجال الطيران والإلمام بالتدابير والأهداف. وينبغي تكييف هذه البرامج مع الجمهور المقصود بها، حسب الاقتضاء والإمكان.

٣-٧ وينبغي إخضاع جميع الموظفين عند توظيفهم لبرامج التوعية بالأمن الإلكتروني فضلاً عن خضوعهم للتدريب التنشيطي في هذا الصدد. وينبغي تحديد الفترات الزمنية لتكرار برنامج التوعية على أساس مستوى نضج ثقافة الأمن الإلكتروني في المنظمة، ويمكن إعادة النظر فيها بما يتماشى مع تطور مستوى النضج هذا.

٤-٧ ويستصوب الخضوع لبرامج التوعية بالأمن الإلكتروني مرة واحدة على الأقل بشكل شخصي (داخل قاعة دراسة فعلية أو افتراضياً). فالأمن الإلكتروني ليس بالموضوع المألوف لجميع الموظفين، بل قد يصعب استيعابه أحياناً دون توجيه من أحد المهنيين المحترفين. وعلى هذا النحو، فإن التفاعل مع أحد المهنيين المحترفين داخل قاعة الدراسة يُسهِّل فهم المواضيع المُتعلِّقة بالأمن الإلكتروني، ويسمح للمُدرِّب بشرح المفاهيم والعمليات والإجراءات والضوابط بطريقة مبسطة يفهمها الموظفون غير المتخصِّصين فنياً، فضلاً عن شرح الفائدة في تعزيز وضع الأمن الإلكتروني للمنظمة وتأثيره الإيجابي في الإنتاجية الإجمالية للموظفين.

٥-٧ وبعد دورة التوعية/التدريب الأوَّلية الشخصية، قد تنظر المنظمات في استخدام أساليب التعلُّم الإلكتروني (التعلُّم المُدار بالحاسوب) للتدريب المتكرر. وينبغي أن يراعي مثل هذا القرار تطور ثقافة الأمن الإلكتروني في المنظمة، فضلاً عن التغييرات في عمليات الأمن الإلكتروني والضوابط والإجراءات التي أُدخلت في المنظمة من أجل مواكبة تطوُّر مشهد مخاطر الأمن الإلكتروني.

٦-٧ وينبغي أن يضطلع بتنفيذ برامج التوعية بالأمن الإلكتروني أفراد مهنيون يمتلكون المعرفة الفنية المطلوبة. ومع ذلك، فإن أحد التحديات التي تواجه برامج التوعية التقنية هو افتقار مقدمي العروض إلى المهارات الشخصية، حيث تقطع مهارتي التواصل و"البيع" الملائمة شوطاً طويلاً في إشراك الموظفين وضمان تأييدهم ودعمهم لثقافة الأمن الإلكتروني. وبناءً على ذلك، ينبغي للمنظمات أن تكفل تزويد مُقدِّمي برامج التوعية بالقدر اللازم من المعرفة التقنية والمهارات الشخصية على حد سواء لغرس التغيير المطلوب في سلوك الموظفين لدعم تبنّيهم لثقافة الأمن الإلكتروني.

٧-٧ ينبغي أن يتضمن البرنامج النموذجي للتوعية بالأمن الإلكتروني المواضيع التالية:

أ) التعريف بالغرض من برنامج التوعية؛
ب) آليات الإعلام والاتصال الموجودة لدى المنظمة؛
ج) نظرة عامة على المخاطر الإلكترونية على الطيران المدني وعواقبها المحتملة (بما في ذلك أمثلة عليها)؛
د) ضوابط الأمن الإلكتروني وعملياته وإجراءاته؛
هـ) دور العنصر البشري في حماية المنظمة من المخاطر الإلكترونية؛
و) أهمية تذكير الموظفين بعضهم لبعض بمبادئ الأمن الإلكتروني التنظيمية عند ملاحظة أفعال من الزملاء تنم عن عدم الالتزام؛
ز) نظرة عامة على أساليب الاستغلال المختلفة التي قد تستهدف الناس وعواقبها (بما في ذلك أمثلة عليها)؛
ح) كيفية التعرُّف على الأنشطة الإلكترونية المشبوهة وتحديدها؛
ط) تأثير الرضا عن الذات في المنظمة (بما في ذلك أمثلة على ذلك)؛
ي) مبادئ النظافة الإلكترونية؛
ك) التعامل السليم مع البيانات والمعلومات الحسَّاسة؛
ل) آليات الإبلاغ، وكيفية استخدامها، وآليات المتابعة.

٨-٧ كما ينبغي استخدام حملات التوعية بالأمن الإلكتروني بشكل دوري، كتذكير، من أجل تعزيز معارف ومهارات الموظفين. وهناك أدوات مختلفة متاحة لهذا الغرض تتضمَّن ما يلي:

أ) *الأدوات الورقية* – مثل الملصقات والكتيبات ...الخ. حيث يكفل هذا النوع من مواد الاتصال سهولة التوزيع والاستيعاب. غير أنها أدوات سلبية، ويلزم تحديثها بشكل تكراري (وطباعة جديدة مع كل تحديث)؛

ب) الأدوات الإلكترونية عبر الإنترنت – مثل البريد الإلكتروني والنشرات الإخبارية الإلكترونية والرسائل الإلكترونية على شاشات التوقف وشبكات العمل الداخلي الإلكترونية ومقاطع الفيديو القصيرة وصفحات الأسئلة الشائعة والتعلُّم الإلكتروني (التعلُّم المُدار بالحاسوب) ...إلخ. والميزة الرئيسية لهذه الأدوات بالمقارنة مع الأدوات الورقية هي القدرة على الوصول إلى المنظمة بأكملها وسهولة تحديثها وإعادة نشرها من حيث الموارد وانخفاض تكلفة إنتاجها.

٨- نُظُم الإبلاغ

٨-١ من الأركان الأساسية لثقافة الأمن الإلكتروني وضع وتنفيذ نظام داخلي للإبلاغ عن الأمن الإلكتروني، بحيث يسمح للمنظمة بإدارة مخاطرها الإلكترونية بشكل استباقي، ويُمكِّنها من قياس تطور وضعية الأمن الإلكتروني للمنظمة، وتحديد احتياجات الموظفين من التوعية والتدريب والتخطيط لها، وتكييف عملياتها الداخلية وضوابطها وتدابيرها بما يتماشى مع تطوُّر اتجاهات الأمن الإلكتروني ومع مستوى نضج ثقافة الأمن الإلكتروني.

٨-٢ وتجمع نُظُم الإبلاغ عن الأمن الإلكتروني عناصر من كل من نظام الإبلاغ عن سلامة الطيران و نظام الإبلاغ عن أمن الطيران. وعلى هذا النحو، فإنها تتناول مجالين: المجال الأول هو الإبلاغ عن الأخطاء/الإجراءات الذاتية التي لا تتماشى مع السياسات والعمليات التنظيمية المُتعلِّقة بأمن المعلومات، أما المجال الثاني، فهو الإبلاغ عن السلوك المشبوه/الخاطئ للموظفين الآخرين.

٨-٣ والمنظمات مدعوة، عند تطوير آلية الإبلاغ عن الأمن الإلكتروني، إلى الاستفادة من التجربة المكتسبة من تطوير وتنفيذ نُظُم الإبلاغ عن سلامة الطيران وعن أمن الطيران.

٨-٤ ينبغي النظر في العناصر التالية عند تنفيذ نظام للإبلاغ عن الأمن الإلكتروني:

أ) الحفاظ على سرية المعلومات الشخصية، إذ لا يتعين جمع البيانات الشخصية و/أو تخزينها. وعندما يجري جمع البيانات الشخصية فلا يجب استخدامها إلا للحصول على توضيح أو على مزيد من المعلومات حول الحادث المُبلغ عنه أو تقديم تعليقات لمقدِّم البلاغ.

ب) من أجل ضمان سرية المعلومات الشخصية، يجب وضع سياسة واضحة تحدد وتُحاسب الشخص (الأشخاص) المكلَّفين بإدارة المعلومات التي جرى جمعها وصيانتها وحماية سريتها وتحليلها ومتابعتها؛

ج) توفير التدريب الملائم لجميع الموظفين حول كيفية استخدام نظام الإبلاغ؛

د) تنفيذ ثقافة العدل في الإبلاغ عن الأمن الإلكتروني، وتوفير التوعية الملائمة لجميع الموظفين حول كيفية عمل ثقافة العدل بحيث يشعرون بالارتياح إزاء توفير المعلومات؛

هـ) تنفيذ برنامج تحفيزي، حسب الاقتضاء، يهدف إلى تشجيع الموظفين على الإبلاغ عن أخطائهم الخاصة وكذلك عن أي سلوك إلكتروني مثير للارتياب يلاحظونه.

ثقافة العدل

٨-٥ ينبغي للمنظمات أن تشجع موظفيها على الإبلاغ عن وقائع الأمن الإلكتروني من خلال تبنِّي ثقافة العدل. فثقافة العدل مفهوم يجري اتباعه في الإبلاغ عن السلامة، ويمكن أن يكون لذلك قيمة كبيرة في تعزيز ثقافة الأمن الإلكتروني.

٨-٦ في سياق الإبلاغ عن الأمن الإلكتروني، تشجع ثقافة العدل جميع الموظفين على الإبلاغ عن الوقائع والأخطاء المُتعلِّقة بالأمن الإلكتروني. فهي عبارة عن بيئة يفهم فيها الجميع أنهم سيُعاملون بإنصاف على أساس أفعالهم وليس نتائج أفعالهم. وفي بيئة ثقافة العدل، يدرك جميع الموظفين بوضوح أنه ليس من العدل المعاقبة على جميع الأخطاء بغض النظر عن الظروف، ويفهمون أيضاً

أنه من غير المقبول في الوقت ذاته توفير حصانة شاملة من العقاب نظراً لأن هناك بعض الأعمال التي قد يكون وراءها مقاصد خبيثة، أو التي تكون نتيجة لإهمال محض و/أو بسبب عدم الاكتراث. وعلى هذا النحو، فمن الضروري تحديد الخط الفاصل بين الإجراءات المقبولة والإجراءات غير المقبولة عند تصميم ثقافة العدل.

٨-٧ لا تُحدِّد ثقافة العدل مسؤوليات الموظفين تجاه منظماتهم فحسب، بل تُحدِّد أيضا مسؤوليات الإدارة تجاه الموظفين. وينبغي إدراج هذه المسؤوليات في سياسة ينبغي بمقتضاها للإدارة العليا للمنظمة أن تقوم بما يلي:

أ) تشجيع الموظفين على ممارسة النظافة الإلكترونية والالتزام بالاعتراف بجهودهم في دعم المنظمة من أجل إدارة المخاطر الإلكترونية؛
ب) الالتزام بتزويد جميع الموظفين بالقدر الكافي من إجراءات الأمن الإلكتروني والتوعية والتدريب والتعليم من أجل دعمهم في أداء واجباتهم؛
ج) تحمُّل المسؤولية عن أي واقعة ناجمة عن نقص الوعي أو عن السرعة في معالجة خطر إلكتروني معين؛
د) تشجيع الموظفين على الإبلاغ عن الوقائع أو المخاطر أو الأخطاء الإلكترونية أو أي سلوك مشبوه يشهدونه دون خوف من الانتقام.

مراقبة الجودة

٨-٨ ينبغي للمنظمات أن تنفذ برامج لمراقبة الجودة، تكون مُصمَّمة لرصد التنفيذ الفعَّال لتدابير الأمن الإلكتروني. ويمكن لبرامج مراقبة الجودة أن تكون أداة فعَّالة من أجل إبقاء الموظفين في حالة تأهب والتزام بمبادئ ثقافة الأمن الإلكتروني. إذ إن وتيرة ضوابط الجودة وصرامتها لها تأثيرها الإيجابي في الموظفين من خلال البرهنة على التزام الإدارة بأهداف الأمن الإلكتروني والامتثال لها.

٨-٩ ينبغي تنفيذ ضوابط دورية لجودة آليات الإبلاغ المُطبَّقة في إطار برامج مراقبة الجودة.

٩- الاستعراض والتحسين بشكل مستمر

٩-١ ينبغي للمنظمات أن تضع إطاراً لمؤشرات الأداء يهدف إلى تقييم تأثير التدابير المُطبَّقة في ثقافة الأمن الإلكتروني، وكذلك لتحديد الفجوة القائمة بين النتائج المتوخاة والواقعية بشأن ثقافة الأمن الإلكتروني.

٩-٢ ونظراً لوجود بعض عناصر ثقافة الأمن الإلكتروني التي قد لا تُلاحظ مباشرة، فيمكن استخدام مجموعة من المؤشرات الممكنة لقياس مدى فعالية ثقافة الأمن الإلكتروني. وقد تشمل هذه التدابير ما يلي:

أ) إحصاءات عن الوقائع المُبلغ عنها (تُعرض مُقارنة ببيانات مستخرجة من سجلات المنظمة) لقياس أداء الموظفين في مجال الأمن الإلكتروني، ومستوى وعيهم، والتقدُّم المُحرَز بشأن تعزيز الإبلاغ عن الأمن الإلكتروني؛
ب) نتائج الدورات التدريبية التنشيطية؛
ج) نتائج محاكاة الهجمات الخبيثة بغرض اختبار استجابة الموظفين؛
د) الاستبيانات والمقابلات.

١٠- وجود بيئة عمل إيجابية

١٠-١ إن وجود بيئة عمل إيجابية بشكل عام قد تؤثر أيضاً بشكل كبير في مدى التزام الموظفين بثقافة الأمن الإلكتروني، وتعزيز أداء الأمن الإلكتروني.

١٠-٢ وينبغي أن تشمل بيئة العمل الإيجابية ما يلي كحد أدنى:

أ) مشاركة الموظفين في عمليات صنع القرار (مثل تقديم اقتراحات لتحسين برامج التدريب على إذكاء الوعي بالأمن الإلكتروني)؛

ب) تخصيص الوقت الكافي للموظفين لاستكمال التدريب على النظافة الإلكترونية السليمة؛
ج) آلية لتقدير الأداء الجيد (أي برامج الحوافز و/أو المكافآت)؛
د) توفير التعليقات للموظفين بشأن الاقتراحات وتقارير الأمن الإلكتروني؛
هـ) تحديد أهداف واضحة وقابلة للتحقيق والقياس في ما يتعلق بوقائع الأمن الإلكتروني، وتقديم تعليقات دورية للموظفين حول إنجاز المنظمة في هذا الصدد؛
و) توفير ما يلزم من إجراءات وتوعية وتدريب وأدوات من أجل تمكين الموظفين من أداء واجباتهم؛
ز) تزويد الموظفين بالمستويات المناسبة من الاستقلالية والمسؤولية.

— انتهى —