تحقيق المرونة في الأمن الإلكتروني من خلال نهج قائم على تحليل المخاطر

نهج قائم على تحليل المخاطر لتنفيذ برامج الحوكمة الإلكترونية الفعَّالة في ظل بيئة محفوفة بتهديدات تتزايد باستمرار

EY
نبني عالماً أفضل للعمل

القمة العالمية للحكومات 2023

المقدمة

تعمل القمة العالمية للحكومات على تحليل مستويات الحاجة إلى تنفيذ برامج فعالة للحوكمة السيبرانية والمخاطر والامتثال داخل المؤسسات الحكومية. وجدير بالذكر أن المخاطر السيبرانية الحديثة باتت تهدد المنظومة الحكومية بأكملها، الأمر الذي يوجب بأن يكون الأمن السيبراني من الأولويات الرئيسية والحاسمة بالنسبة للشركات. ويجب أن تتمتع تقنيات الجيل التالي بأفضل الممارسات والحلول الذكية، كما ينبغي لها أن تتضمن منهجيات فعّالة لضمان تحقيق المرونة السيبرانية.

وتستعد الهيئات الحكومية ومؤسسات القطاع العام لدخول عصر من التحول الرقمي، يتطلب وجود آلية متكاملة تراعي الجوانب المتعددة للمؤسسات. ومن المهم أن ننتقل من مفهوم الأمن السيبراني إلى مفهوم المرونة السيبرانية لنعزز استعدادنا لمواجهة التعقيدات في البيئة الجيوسياسية غير المستقرة التي نشهدها من حولنا اليوم.

الفهرس

القسم الأول: الملخص التنفيذي	04
القسم الثاني: الجغرافيا السياسية والمجال الرقمي: تأثير الفضاء الإلكتروني على الحكومة والجهات الحكومية	06
القسم الثالث: تطور البيئة التنظيمية للأمن الإلكتروني من أجل مكافحة آثار هشاشة الأوضاع في المشهد الجغرافي السياسي	10
القسم الرابع: نهج حوكمة فعال لإدارة المرونة في الأمن الإلكتروني	16
القسم الخامس: تطبيق نهج سريع لإدارة المخاطر الإلكترونية وتلبية متطلبات الامتثال	24
القسم السادس: إدارة استمرارية الأعمال وتعريف الاستجابة واستراتيجيات التعافي	34
القسم السابع: الخاتمة	36
دعوة للعمل	38
المراجع	40
المساهمون	41

القسم الأول

الملخص التنفيذي

تستند قدرة أي جهة على تحقيق أهدافها إلى مقدرتها على التغلب على المخاطر التي تواجهها بصورة فعَّالة، بما في ذلك المخاطر الإلكترونية. ومن المؤسف أن الإدارة التنفيذية ليست ملمة بمدى كفاءة إدارة المخاطر الإلكترونية في جهاتها ومدى مرونة عملياتها.

قدَّم الاستطلاع العالمي لأمن المعلومات، الذي أجرته "إرنست ويونغ" في العام 2021 عرضاً موجزاً حول هذا الأمر حيث ذكر أن 56.2٪ من المدراء التنفيذيين الذين شملهم الاستطلاع لا يعلمون ما إذا كانت دفاعاتهم قوية بما يكفي للتصدي لاستراتيجيات الاختراق الجديدة التي يتبعها القراصنة أم لا.[1]

ورغم القلق المتزايد بشأن الحفاظ على المرونة في الأمن الإلكتروني، فقد أدى الضغط من أجل سرعة تحقيق التحول الرقمي لدفع الجهات، لا سيما في القطاع الحكومي، إلى إهمال عمليات الأمن الإلكتروني. وربما لم يكن من قبيل المصادفة تزامن ذلك مع تزايد الهجمات الإلكترونية، لا سيما من الجهات التخريبية التي تقف وراء التهديدات الجغرافية السياسية مثل المجموعات التي ترعاها الحكومات والجهات الحكومية.

تعمل جميع الجهات الحكومية بشكل جوهري على أساس الثقة. لذا يتعين على هذه الجهات إظهار تفانيها المتواصل في الحفاظ على السرية، وتأكيد توفر الأنظمة والخدمات، والحفاظ على أمن البيانات من أجل كسب ثقة المواطنين والحفاظ عليها. ومن ثم تشكل الهجمات الإلكترونية تهديداً لم يسبق له مثيل للحكومة والقطاع الحكومي. ومن الضروري وضع الأمن الإلكتروني في صميم استراتيجية أي جهة حكومية، وذلك من خلال وضع برنامج فعَّال للحوكمة الإلكترونية وإدارة المخاطر والامتثال، مدفوع بنهج دمج الأمن في التصميم (SbD) الذي يعتمد التفكير القائم على أساس تقييم المخاطر من بداية أي مشروع.

أتاحت لنا معارف فرق إرنست ويونغ المتعددة الاختصاصات وكفاءاتها الأساسية في الحوكمة الإلكترونية وإدارة المخاطر والامتثال مساعدة العديد من الجهات الحكومية في وضع منهجيات فعَّالة لضمان المرونة في الأمن الإلكتروني. فقد أصبحت الجهات الحكومية الرائدة تبني منهجيات تراعي مناخ الأعمال، إلى جانب مشهد المخاطر الجغرافية السياسية، حيث بات من الواضح أن الحرب الهجينة، مثل الهجمات الإلكترونية، هي الواقع الجديد، وأن الجغرافيا السياسية والأمن الإلكتروني مرتبطان ارتباطاً وثيقاً.

وبينما لا توجد جهة محصنة ضد الهجمات الإلكترونية، فإن الجهات الحكومية التي تمتلك أنظمة دفاع إلكتروني قوية وأنظمة لحماية البيانات وتلك التي تراعي اتباع نهج قائم على أساس تقييم المخاطر لتحقيق الأمن الإلكتروني، من المرجح أن تكون أكثر مرونة. إن النهج القائم على تقييم المخاطر من أجل تحقيق الأمن الإلكتروني يتيح للجهات الحكومية التركيز على حماية أصول المعلومات العالية القيمة والتخفيف من المخاطر الأشد تأثيراً، ومن ثم تقليص المساحة المعرضة للهجوم. ويتطلب تنفيذ هذا النهج اتباع آلية متكاملة تراعي الجوانب المتعددة للجهة (مثل أنواع الأصول وتعقيد العمليات) ومنهجية تدريجية تشمل فهم بيئة الأعمال والتكنولوجيا، وتصنيف أصول التكنولوجيا، وتحليل المخاطر أو التهديدات، وتقييم تصميم التحكم، وتنفيذ خيارات معالجة المخاطر.

يوضح هذا التقرير ضرورة تركيز الحكومة وجهات القطاع الحكومي على قدرات المرونة في الأمن الإلكتروني التي تقلل من تأثير أي هجمة إلكترونية ناجحة، وتقديم النهج المذكور أعلاه القائم على تقييم المخاطر من أجل تنفيذ برامج شاملة وفعَّالة للحوكمة الإلكترونية وإدارة المخاطر والامتثال تشمل في المقام الأول تقييمات المخاطر الإلكترونية مدعومةً بتقييمات فنية شاملة، مثل تقييمات مواطن الضعف واختبارات الاختراق ومراجعات إعدادات الأصول المهمة.

> إن النهج القائم على تقييم المخاطر من أجل تحقيق الأمن الإلكتروني يتيح للجهات الحكومية التركيز على حماية أصول المعلومات العالية القيمة والتخفيف من المخاطر الأشد تأثيراً، ومن ثم تقليص المساحة المعرضة للهجوم

القسم الثاني

الجغرافيا السياسية والمجال الرقمي: تأثير الفضاء الإلكتروني على الحكومة والجهات الحكومية

عند النظر إلى التطورات التكنولوجية الحديثة وترابط العالم، سندرك أنه لم يعد بإمكاننا فصل عالم التكنولوجيا عن عالم الأعمال وإغفال أهمية التكنولوجيا الحديثة للعمليات الحاسمة. فقد أصبحت تكنولوجيا المعلومات والتكنولوجيا التشغيلية عنصراً أساسياً لا غنى عنه في مختلف القطاعات. وباتت العمليات تعتمد بشكل كبير على التكنولوجيا التشغيلية أو أنظمة التحكم الصناعية، بما في ذلك العمليات الحيوية في القطاعات الأساسية أو البنية التحتية للشبكات الحيوية (CNI)، مما أدى إلى أن تصبح هذه التقنيات مستهدفة بشكل رئيسي من المهاجمين التابعين للدول. وبينما يوجد العديد من الجهات ذات النوايا الخبيثة في الفضاء الإلكتروني، فإن الجهات التخريبية التي ترعاها الحكومات وتقف وراء التهديدات قادرةٌ على إلحاق أعلى درجات الضرر بالجهات الحكومية والقطاع الحكومي من خلال مستوى تطور هجماتها. تنفذ الجهات التخريبية التي ترعاها الحكومات وتقف وراء التهديدات عمليات أمنية نيابةً عن الدولة، وفي أغلب الحالات يكتنف الغموض عملياتها.

ويمكن أن يُعزى انتشار الجهات التخريبية التي ترعاها الحكومات إلى عدم استقرار البيئة الجغرافية السياسية الحالية. وفي مثل هذه الحالة المتقلبة للشؤون الدولية، نتوقع ملاحظة المزيد من العمليات الإلكترونية المدفوعة بالجغرافيا السياسية على المدى القريب والمتوسط مستقبلاً. ومن ثم فإن زعزعة الاستقرار واستمرار تجاوز الحد فيما يتعلق بالنشاط الإلكتروني الضار قد يؤدي أيضاً إلى إلحاق المزيد من الضرر. وقد لوحظ ذلك في الآونة الأخيرة لا سيما عندما تعرض عدد من أكبر شركات البنية التحتية الوطنية الحيوية في جميع أنحاء الاتحاد الأوروبي لهجمات إلكترونية خلال الحرب في أوكرانيا. وقد ورد في تقرير الدفاع الرقمي من مايكروسوفت لعام 2022 على لسان الشركة المتخصصة في صنع البرمجيات أن الهجمات الإلكترونية المتصلة بأنشطة الدولة والتي تستهدف البنية التحتية الحيوية في جميع أنحاء العالم ارتفعت من 20٪ إلى 40٪ بين عامي 2021 و2022.[2]

وخلال هذه الفترة، أخذ نوعان من البرمجيات الخبيثة المتطورة المصممة لاستهداف أنظمة التحكم الصناعية (ICS) في الانتشار بشكل متزايد، وهما (Pipedream Incontroller) وIndustroyer، وكان تأثيرهما الأكبر في أوكرانيا، حيث تسببا في وقوع أضرار وأعطال في البنية التحتية للشبكات الحيوية الخاصة بالطاقة والمرافق والاتصالات السلكية واللاسلكية والعديد من الأنظمة الأخرى. وإلى جانب ذلك، استغلت جماعات الجريمة المنظمة التي ترعاها الحكومات الثغرات الأمنية (على وجه التحديد ثغرات الهجوم الفوري) لتنفيذ الهجمات الإلكترونية. ويعد ProxyLogon وأداة Fatedier Reverse Proxy وProxyShell من هذه الثغرات الأمنية المسجلة وفقاً لتقرير التهديدات العالمية الصادر عن شركة "كراود ستريك" في عام 2022.[3] فمثلاً اكتُشف ProxyShell أثناء عملية تجسس إلكتروني استهدفت مقدمي خدمات الاتصالات في الشرق الأوسط بواسطة إحدى مجموعات التهديدات المستمرة المتقدمة (APT) في عام 2022.[4]

قد تمتد الحرب الإلكترونية أيضاً إلى سباق التسلح بين الدول، مما قد يؤدي إلى اكتساب قدرات عسكرية على نحو تنافسي وتنافس الجهات التخريبية التي ترعاها الحكومات على أفضل التقنيات وأقواها. في عام 2022، حصلت مجموعات التهديدات المستمرة المتقدمة على معلومات تكنولوجية وملكية فكرية (IP) لصالح الصناعات المملوكة للدولة. مجموعة Winnti (جماعة التهديدات المستمرة المتقدمة رقم 41) على سبيل المثال، هي حملة عالمية للتجسس الإلكتروني تستهدف الشركات المصنعة في جميع أنحاء أمريكا الشمالية وأوروبا وآسيا في مجالات الدفاع والطاقة والطيران والتكنولوجيا الحيوية والصناعات الدوائية (هنريكيز، 2022).[5]

في عالمنا الحاضر، لا يمكن تفادي الحرب الإلكترونية. حيث إن زعزعة الاستقرار في العالم والتوترات السياسية وحتى الهجمات الإلكترونية بشكل عام، تُلزِم الدول بإعادة النظر في استراتيجياتها وإدراج الأمن الإلكتروني ضمن الأدوات الأمنية للتصدي للهجمات الإلكترونية التي قد يترتب عليها آثار كارثية في القطاعات الحيوية.

وقد حدثت في شهر أبريل 2022 هجمة إلكترونية كبيرة في كوستاريكا، حيث تمكن المهاجمون من اختراق وزارة المالية وتسببوا في شل حركة شبكة الوزارة مطالبين بفدية قدرها 10 ملايين دولار أمريكي لإعادة إمكانية دخول الشبكة إلى الحكومة (ريد، 2022). تعرض خط أنابيب نفط أمريكي مكرر ينقل منتجات بترولية مكررة من هيوستن بولاية تكساس إلى الأجزاء الشرقية من الولايات المتحدة، إلى هجوم برمجيات فدية في شهر مايو من عام 2021، ونجم عن هذا الهجوم تعطل أنظمة الكمبيوتر وحصول تداخل في عمليات خط الأنابيب هذا. وعانى بعض عملاء هذا الخط من نقص في إمدادات الوقود، كما تركت أخبار هذا الهجوم السيبراني آثاراً سلبية على العملاء الذين ينتجون الوقود لصالح محطات الوقود. وأدت تلك المخاوف إلى حالة من القلق من نقص إمدادات الوقود مما أدى بدوره إلى حالة من هلع الشراء.

وقد تسببت الطوابير الطويلة في محطات الوقود في العديد من الولايات إلى حدوث بعض النقص وزيادات في أسعار الوقود. ويمكن أن يترتب على هذه الهجمات عواقب وخيمة تبعاً لحجم الهجوم ونطاقه.

وقد تغيرت مفاهيم الحرب والسياسة في العصر الرقمي ويزداد تعقيد الهجمات مع استخدام التكنولوجيا الحديثة، مثل الحوسبة الكمية وإنترنت الأشياء (IoT) وتقنية "البلوك تشين" (Blockchain). ومن ثم تتطلب طبيعة هذه المخاطر تعاون الحكومات مع القطاع العام من أجل وضع اللوائح والسياسات والإجراءات لمواجهة التهديدات الإلكترونية والقضاء عليها على نحو فعَّال.

> وإلى جانب ذلك، تزايدت عمليات التأثير في عام 2022 لتمكين الحرب الدعائية من إضعاف الثقة والتأثير على الرأي العام لنشر الروايات عبر وسائل الإعلام وقنوات التواصل الاجتماعي التي تدعمها الحكومة وتؤثر عليها.[6]

القسم الثالث

تطور البيئة التنظيمية للأمن الإلكتروني من أجل مكافحة آثار هشاشة الأوضاع في المشهد الجغرافي السياسي

في ظل الأوقات العصيبة، وبينما يستعيد العالم توازنه في ضوء الدروس المستفادة خلال جائحة كوفيد-19، يجب ألا يغيب عن أذهاننا أن البيئة في تغير مستمر ومليئة بالتحديات. فقد شهدنا خطوات لم يسبق لها مثيل في التحول الرقمي على مستوى الجهات الحكومية والخاصة وزيادة استخدامها للتقنيات من أجل تحقيق الأهداف الاستراتيجية. و شهدنا في عام 2022 كيف تسببت التوترات الجغرافية السياسية في كشف حقيقة الحرب الإلكترونية كما بينت لنا الحرب في أوكرانيا ومنطقة الشرق الأوسط، لا سيما في المملكة العربية السعودية والإمارات العربية المتحدة وقطر، حيث كان لها تأثير على الصناعات والاقتصادات. وقد شجعت هذه السيناريوهات تهديدات الأمن الإلكتروني على النمو والتطور سريعاً، على الساحة الوطنية والعالمية. ومن ثم أصبحت الحكومة بوصفها صانعة للسياسات وجهة منفذة تتمتع بدور حاسم. تواجه تحدياً في سبيل إيجاد بيئة آمنة ومرنة، تتيح للحكومة والقطاع العام، إلى جانب مقدمي خدمات البنية التحتية للقطاعات الحيوية، أن تضمن للمواطنين نمط حياة آمن في ظل الاعتماد المتنامي على الإنترنت.

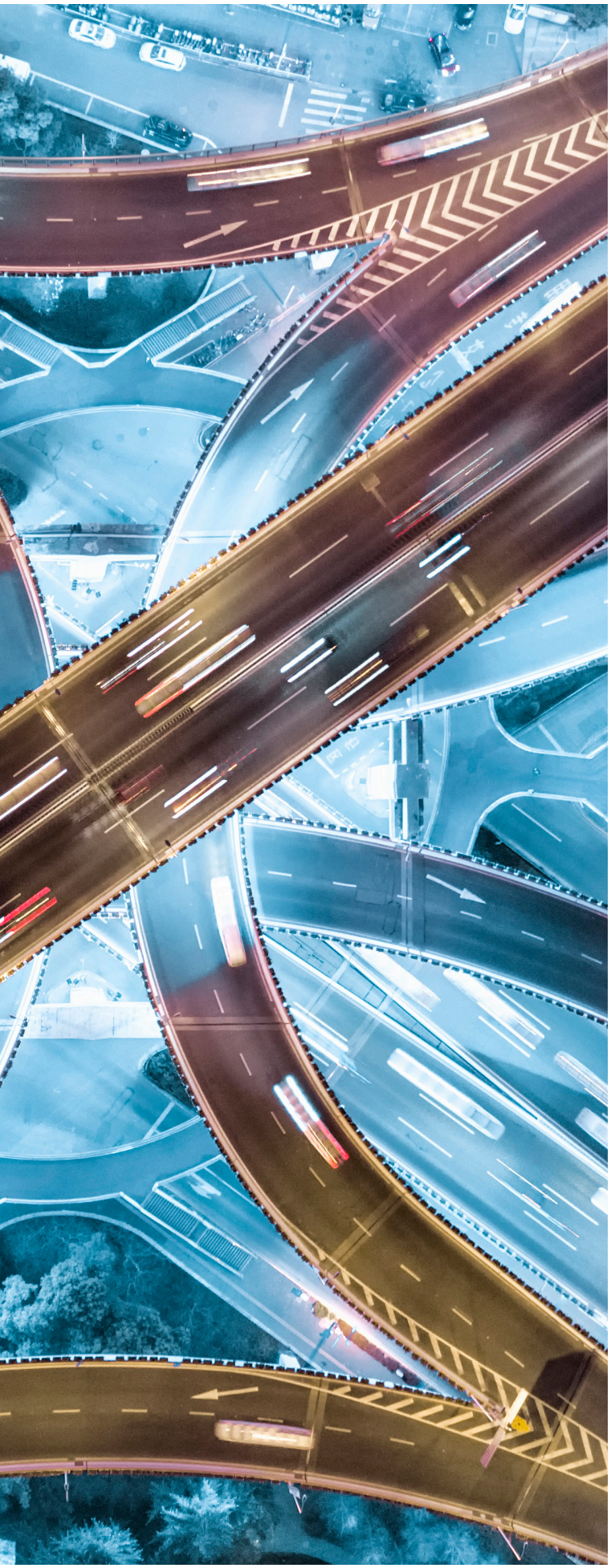
الأطر التنظيمية مقابل مشهد التهديدات الناشئة

مع مشهد التهديدات المتطور دائماً، قد لا تكون الإرشادات التقليدية بشأن أفضل ممارسات الأمن الإلكتروني كافية لمواجهة التهديدات. وهذا يدفع سلطات الدولة إلى وضع وتطبيق القواعد التنظيمية التي من شأنها أن تعزز تنفيذ مرونة الأمن الإلكتروني وإدارتها لمكافحة مخاطر الجيل التالي. عندما نتحدث عن مرونة الأمن الإلكتروني، يمكننا أن نتصور بيئة توفر منظومة إلكترونية آمنة لتشمل البنية التحتية الأساسية ودعم الصناعات للاستمرارية والتعافي من الهجمات الإلكترونية. ويمكن للأطر التنظيمية الوطنية للأمن الإلكتروني التي تغطي موضوعات إدارة المخاطر وتحليل التهديدات الإلكترونية أن تساعد الحكومات في مكافحة التهديدات الناشئة.

إضافة إلى ذلك، يجب أن تكون القواعد التنظيمية قادرة على خلق بيئة مفتوحة تسمح بتبادل المعلومات والتعاون القوي وتشجع عليهما على المستويين الوطني والصناعي. وقد تم توضيح ذلك من قِبل الفريق العامل المفتوح العضوية التابع للأمم المتحدة (OEWG) المعني بالتطورات في مجال المعلومات والاتصالات السلكية واللاسلكية، في مارس 2021. صادق الفريق على تقرير يحتوي على توصيات بشأن الأمن الإلكتروني وتم اعتماده من قِبل جميع البلدان بالإجماع.

الحرب في أوكرانيا ومساهمتها في التهديدات الإلكترونية العالمية

أظهرت الحرب في أوكرانيا نوعية جديدة من حروب القرن الحادي والعشرين. فقد أسفرت عن عددٍ من التداعيات العالمية التي امتدت إلى الفضاء الإلكتروني. أدى التصعيد المستمر إلى تفاقم ظاهرة "الهاكتفيزم"، التي تعني اختراق شخص ما لنظام الكمبيوتر لأغراض سياسية أو اجتماعية، والحرب الإلكترونية التي هددت أيضاً من هم خارج حدود أوكرانيا. تُعد الحرب في أوكرانيا تذكيراً للدول الأخرى بتعزيز دفاعاتها في مجال الأمن الإلكتروني في حال زيادة التوتر داخل أراضيها ومساسه بسياساتها المحلية والخارجية. في ألمانيا، يتم تعزيز مرونة الأمن الإلكتروني بين الشركات التي تقدم خدمات حيوية مثل النقل والطعام والمرافق لمكافحة أي تهديدات محتملة جراء الحرب في أوكرانيا. من ناحية أخرى، كانت فنلندا مبدعة في الدعوة إلى المرونة الإلكترونية من خلال تقديم نظام قسائم من شأنه أن يمول الشركات لتحسين قدراتها الأمنية استجابةً للحرب في أوكرانيا ومحاولة الدولة الانضمام إلى منظمة حلف شمال الأطلسي (الناتو).



> في ألمانيا، يتم تعزيز مرونة الأمن الإلكتروني بين الشركات التي تقدم خدمات حيوية مثل النقل والطعام والمرافق لمكافحة أي تهديدات محتملة جراء الحرب في أوكرانيا

إدارة المخاطر بوصفها متطلباً أساسياً

إن الهدف المتمثل في وجود بيئة تتمتع بالمرونة في الأمن الإلكتروني يستدعي من الحكومات توفير أساليب منظمة لقياس قدرة الجهات الحكومية على الحماية من الهجمات الإلكترونية. لقد رأينا الهيئات التنظيمية تعيد النظر في الإرشادات الحالية لديها المتعلقة بإدارة المخاطر للتأكد من أنها محدثة، لدعم الصناعات والجهات الحكومية في مكافحة التهديدات الإلكترونية. تحتاج الهيئات التنظيمية الوطنية إلى النظر في مجالات التركيز الرئيسية التالية بوصفها جزءاً من أطر الأمن الإلكتروني التي يتم تحديدها:

- المساءلة الشاملة: المرونة عمل جماعي، حيث تحتاج القواعد التنظيمية إلى تفويض الجهات الحكومية للتأكد من أن المتخصصين في التشغيل أو الأمن الإلكتروني ليسوا وحدهم من يضمنون المرونة، بل الأطراف المعنية الداخلية الأخرى أيضاً، بما في ذلك الإدارة التنفيذية المباشرة للشركة وإدارة الموردين والخطان الثاني والثالث والشؤون القانونية ومجلس الإدارة، وغير ذلك. كما، ينبغي تشجيع الجهات الحكومية على وضع وتنفيذ استراتيجية مرونة إلكترونية منسقة ومتعددة التخصصات بصورة فعَّالة واختبارها على أساس دوري من خلال عمليات المحاكاة.

- إدارة المخاطر: لا بد للقواعد التنظيمية أن توفر سبلاً للجهات الحكومية لتضمين متطلبات المرونة في الأمن الإلكتروني في إطار تحمل المخاطر. في هذا السياق، يحتاج خط الدفاع الثاني إلى مجموعة فعَّالة من المقاييس لتقييم مخاطر المرونة في الأمن الإلكتروني. قد تأتي العديد من هذه المقاييس من الخط الأول، لكن الخط الثاني يحتاج إلى مقاييسه الخاصة، خصوصاً لتقييم المخاطر الإلكترونية للجهات الحكومية على المستوى الإجمالي.
- التدقيق الداخلي: يلعب خط الدفاع الثالث (التدقيق الداخلي) دوراً رئيسياً في التحقق والمراجعة. النهج الذي يتبعه الخط الثالث للتحقق من فاعلية الإطار الإلكتروني (الأطر الإلكترونية) المعتمَد من قبل الخطين الأول والثاني لتقييم مخاطر المرونة في الأمن الإلكتروني وإدارتها، ضروري لضمان قدرة المرونة على مقاومة الهجمات الإلكترونية.

في 13 مايو 2022، قام مجلس الاتحاد الأوروبي والبرلمان الأوروبي بمراجعة وتحديث التوجيه الحالي لأمن الشبكات والمعلومات (NIS) ليصبح توجيه أمن الشبكات والمعلومات NIS2. يضع التوجيه الجديد "خط أساس لإدارة مخاطر الأمن الإلكتروني والتزامات تقديم التقارير عبر القطاعات الحيوية". وسيتم الاعتراف بالاتفاقية في جميع المناطق المشمولة على أمل وضع تدابير استباقية للتخفيف من حدة التهديدات في مختلف المجالات. في الولايات المتحدة، أصدر المعهد الوطني للمعايير والتكنولوجيا (NIST) نسخة منقحة من ممارسات إدارة مخاطر الأمن الإلكتروني لسلاسل التوريد للأنظمة والجهات الحكومية.[7] يركز الإصدار المنقح على مساعدة الشركات في فهم طرق تحديد مخاطر الأمن الإلكتروني وتقييمها والاستجابة لها على امتداد سلاسل التوريد في كافة أنحاء الجهات الحكومية. إضافةً إلى ذلك، نشرت وزارة التجارة الأمريكية قاعدة مقترحة لتنفيذ القواعد التنظيمية وفقاً للأمر التنفيذي الصادر في مايو 2019، لتحسين سلسلة التوريد لخدمات تكنولوجيا الاتصالات والمعلومات (ICTS).[8] سيعالج هذا المخاوف المتعلقة بتصميم المنتج وتطويره وتصنيعه وتوريده والتحكم في خدمات تكنولوجيا الاتصالات والمعلومات من قِبل الخصوم الأجانب.

انتشار برامج الفدية

يتزايد تهديد برامج الفدية في عام 2022 ولا يزال يمثل خطراً كبيراً على الجهات الحكومية بمختلف أحجامها في جميع القطاعات. يُظهر تقرير عام 2022 الصادر عن وكالة الاتحاد الأوروبي للأمن الإلكتروني (ENISA) حول مشهد تهديدات برامج الفدية كيف أن الجهات الحكومية لا تزال عرضة لهذا النوع من الهجمات وقد خلُص إلى أن لها تأثيراً مدمراً على هذه الجهات، خاصة إذا لم تكن مستعدة لمواجهتها.

دفعت المخاطر التي تفرضها برامج الفدية الهيئات التنظيمية والقائمين على تطبيق القانون في جميع أنحاء العالم إلى التعاون في مكافحة هجمات هذه البرامج. في يوليو 2021، بمنتدى الإنتربول الرفيع المستوى المعني ببرامج الفدية، تمحور النقاش حول أن منع برامج الفدية وتعطيلها بشكل فعَّال يقتضيان "اعتماد التعاون الدولي نفسه المستخدم لمكافحة الإرهاب أو الاتجار بالبشر أو جماعات المافيا".[9] وقد دعت المجموعة أجهزة الشرطة في جميع أنحاء العالم لتشكيل تحالف عالمي مع شركاء المجال لوقف النمو المتسارع لبرامج الفدية. كما نشر المركز الوطني للأمن الإلكتروني في المملكة المتحدة (NCSC)، ومركز الأمن الإلكتروني الأسترالي (ACSC)، ومكتب التحقيقات الفيدرالي (FBI)، ووكالة الأمن القومي (NSA)، ووكالة الأمن الإلكتروني وأمن البنية التحتية (CISA) تنبيهاً مشتركاً[10]، يحث الشركات على اتخاذ إجراءات لحماية نفسها من الهجمات.

من ناحية أخرى، لوقف انتشار هجمات برامج الفدية، تم سنُّ التشريعات التي تحظر دفع الفدية في ظل الحرب في أوكرانيا. على سبيل المثال، قام مكتب مراقبة الأصول الأجنبية (OFAC) التابع لوزارة الخزانة الأمريكية بمنع دفع الفدية، بما في ذلك المدفوعات بالعملات الرقمية أو المدفوعات التي يتم تسهيلها من خلال الغير، إلى الأشخاص أو الكيانات الخاضعة للعقوبات.[11] إضافة إلى ذلك، أصدرت شبكة إنفاذ الجرائم المالية، كمحاولة أخرى لمنع دفع الفدية للكيانات الخاضعة للعقوبات، تنبيهاً إلى جميع المؤسسات المالية "للتيقظ ضد محاولات التهرب من العقوبات الموسعة وغيرها من القيود التي تفرضها الولايات المتحدة فيما يتعلق بالحرب في أوكرانيا".[12]

> تعمل الحكومات أيضاً بصورة استباقية لمكافحة برامج الفدية، ففي الولايات المتحدة، أطلق مكتب التحقيقات الفيدرالي وحدة استغلال الأصول الافتراضية (VAXU) لتتبع برامج الفدية وأرباحها.[13]

تجديد الاهتمام بالأمن الإلكتروني الصناعي

مع تزايد أجهزة التكنولوجيا التشغيلية وإنترنت الأشياء، يتطلب مجال الأمن الإلكتروني الصناعي اهتماماً متجدداً من الهيئات التنظيمية. لمكافحة سهولة التأثر المتزايدة لهذا المجال بالهجمات الإلكترونية، وضعت البلدان متطلبات تقنية لتعزيز الضوابط الأمنية على أجهزة التكنولوجيا التشغيلية/إنترنت الأشياء. في أوروبا، أدخل الاتحاد الأوروبي تعديلات على توجيه الاتحاد الأوروبي بشأن المعدات اللاسلكية لعام 2014، بما يضمن أن تكون جميع الأجهزة اللاسلكية آمنة بما فيه الكفاية قبل بيعها. تطلب ذلك من الشركات المصنعة اتباع إجراءات وقائية جديدة للأمن الإلكتروني عند تصميم المنتجات وإنتاجها، وفرض حماية متزايدة للبيانات الشخصية.[14] بينما في الولايات المتحدة، أعيد تقديم تشريع يُعرف باسم قانون الحماية الإلكترونية "Cyber Shield Act" في الكونغرس في 15 مارس 2021. في حال إقراره، سيضع القانون [15] معايير أمان لأجهزة إنترنت الأشياء بناءً على توصيات لجنة استشارية مكونة من خبراء في الأمن الإلكتروني من الحكومة والأوساط الأكاديمية والجهات الخاصة. سيُسمح لمصنعي الأجهزة الذين يستوفون هذه اللوائح بتمييز منتجاتهم بعلامة تشير إلى أنهم استوفوا المعايير وأن منتجاتهم أكثر أماناً. تدرس أستراليا أيضاً تحويل مجموعة من اللوائح الطوعية إلى لوائح إلزامية من شأنها تحديد مجموعة من متطلبات الحد الأدنى

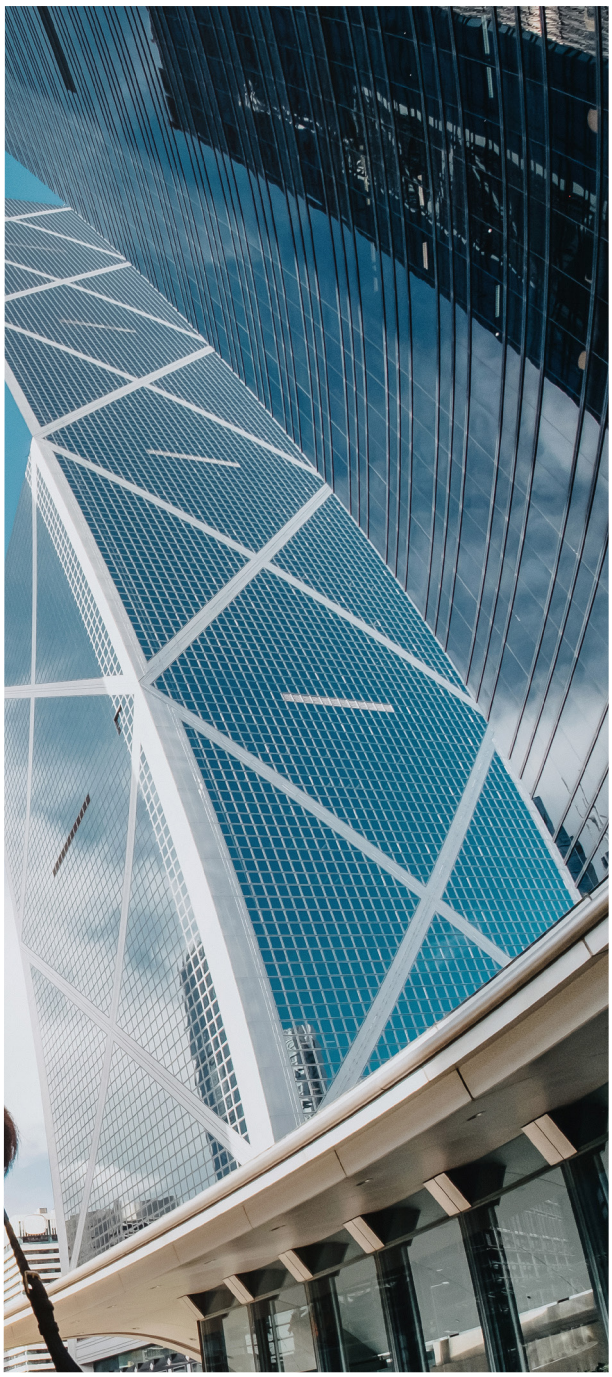
للأمن الإلكتروني فيما يتعلق بالأجهزة الذكية ذات الجودة الاستهلاكية.[16]

تزايد متطلبات الإبلاغ عن الجرائم الإلكترونية

لمزيدٍ من المرونة، تم تقديم لوائح جديدة لتحقيق شفافية أفضل بشأن حوادث الأمن الإلكتروني. بشكل عام، توجد هذه المتطلبات في أنظمة سرية البيانات، حيث توجد متطلبات بشأن إشعارات خرق البيانات. الآن، أدركت الحكومات أن الهجمات الإلكترونية تتجاوز مسألة اختلاس البيانات الشخصية. ففي الولايات المتحدة، تم تمرير قانون الإبلاغ عن الحوادث الإلكترونية للبنية التحتية الحرجة (CIRCIA) في مارس 2022. سيتطلب ذلك من شركات البنية التحتية الحرجة، بما في ذلك الخدمات المالية، الإبلاغ عن حوادث الأمن الإلكتروني، مثل هجمات برامج الفدية، إلى وكالة الأمن الإلكتروني وأمن البنية التحتية (CISA)[17]. إضافةً إلى ذلك، في الإطار الزمني نفسه، اقترحت هيئة الأوراق المالية والبورصات الأمريكية (SEC) قاعدة تطالب الشركات المدرجة في البورصة بإبلاغ هيئة الأوراق المالية والبورصات بحوادث الأمن الإلكتروني، وقدراتها في مجال الأمن الإلكتروني، وخبرة مجلس الإدارة في مجال الأمن الإلكتروني وإشرافها عليه.[18] كما وقع رئيس الولايات المتحدة على "قانون مقاييس أفضل للجرائم الإلكترونية" الذي يحدد المتطلبات الهادفة إلى تحسين الإبلاغ والتتبع الإلكتروني من أجل زيادة تسليط الضوء على نواقل الهجوم وتطور الهجمات.[19]

التحدي المستمر للهيئات التنظيمية

مع زيادة الرقمنة في العالم واستمرار تطور المشهد الجيوسياسي العالمي، لا توجد استجابة قياسية لجميع تهديدات الأمن الإلكتروني. من الضروري أن تضع الحكومات اللوائح والمبادئ التوجيهية التي من شأنها أن تمكن القطاعات والجهات الحكومية من ممارسة المرونة في الأمن الإلكتروني داخل بيئتها الخاصة. يتمثل التحدي في أن تكون الهيئات التنظيمية على دراية بالبيئة الرقمية المتغيرة، وأن تسبق خطواتها خطوات الجهات التخريبية، وأن تُوجِد طريقاً تكون فيه المجالات منفتحة على التعاون والشراكات.



القسم الرابع

نهج حوكمة فعال لإدارة المرونة في الأمن الإلكتروني

في ظل التهديد المتزايد والمتواصل والمشهد الجيوسياسي، أصبح من الضروري الآن للحكومة والجهات الحكومية تعزيز مرونة الأمن الإلكتروني بوصفه جزءاً من مهامها. وبالعودة إلى تعريف المرونة، فهي قدرة الجهة الحكومية على التنبؤ بالأحداث التخريبية ومقاومتها والتعامل معها، وتكييف العمليات في البيئة وإعادة تشكيلها. من خلال تطبيق هذا المفهوم في الأمن الإلكتروني، تهدف المرونة إلى صد الهجمات الإلكترونية المحتملة وضمان التعافي منها، دون فقدان البيانات أو تعرضها للتهديد بعد أي هجوم.

في حين أن ذلك التعريف قد يبدو سهلاً، فإن التحدي الرئيسي يكمن في بناء نظام بيئي حيث يمكن للحكومة ومكوناتها تحقيق عملية مستدامة ومرنة. وبطبيعة الحال، فإن دور الحكومة بوصفها صانعة السياسة هو سن اللوائح التي من شأنها أن توجد المرونة في مجال الأمن الإلكتروني عبر مكوناتها.

إن الطبيعة السريعة التطور لبيئة المخاطر الإلكترونية تؤكد بشكل متزايد على ضرورة أن تتبنى الحكومة والجهات الحكومية نهجاً قائماً على المخاطر للأمن الإلكتروني. لا تستطيع الجهات الحكومية بكل بساطة حماية كل شيء بالدرجة نفسها. الخطوة الأولى هي تنفيذ الحوكمة الإلكترونية بصورة صحيحة. تدرك الحكومات أن الأمن الإلكتروني يمثل خطراً كبيراً، بل ربما الخطر الأكبر، وتعلم أن الخطر يتغير بسرعة تصعب مواكبتها. ومع ذلك، فإنها تكافح لتحديد الكيفية التي يجب أن تتطور بها حوكمتها. من الناحية العملية، ستؤثر مجموعة أوسع من الاتجاهات على التصميم المستقبلي لحوكمة المخاطر الإلكترونية، ومنها القوانين الجديدة للخصوصية والبيانات، وتنفيذ ثلاثة خطوط دفاع للأمن الإلكتروني (3LOD)، والحاجة إلى تضمين الأمن الإلكتروني في الابتكار، والامتثال للوائح الجديدة والتوقعات الإشرافية المعززة. إن تقدير هذه الاتجاهات الأوسع أمر مهم لتصميم أفضل للحوكمة.

	من يمثله؟	ما أدواره في الأمن الإلكتروني؟	ما التحدي الذي يواجهه؟
الخط الأول	وحدات الأعمال وفرق أمن المعلومات الخاضعة للمساءلة المباشرة عن المخاطر الإلكترونية وفهمها وإدارتها.	• قياس ومراقبة وإدارة وتخفيف المخاطر الإلكترونية والثغرات ضمن نطاق تحمل المخاطر الإلكترونية المعتمد من مجلس الإدارة إذا كانت وحدات الأعمال الأمامية تعمل مع فرق أمن المعلومات والأمن الإلكتروني. • تحديد المخاطر الإلكترونية واحتماليات التعرض لها في كل مجال من مجالات الأعمال. • تطوير المعايير والإجراءات التي تنفذ إطار عمل المخاطر الإلكترونية للخط الثاني في سياق مخاطر الأعمال المحددة.	• أن يصبح التفكير في الأمن الإلكتروني جزءاً لا يتجزأ من العمليات اليومية. • أن يحدد الخط الأول (وليس مجموعة الأمن الإلكتروني) المخاطر الإلكترونية بصورة صحيحة، وأن يضع ضوابط قوية ويحافظ عليها.
الخط الثاني	مديرو المخاطر المسؤولون عن إجمالي المخاطر الإلكترونية على مستوى الجهة، والذين يتم منحهم سلطة مستقلة لتحدي نهج الخط الأول تجاه المخاطر الإلكترونية بشكل فعال.	• وضع إطار عمل للمخاطر الإلكترونية والمطالبة بتنفيذ الخط الأول له. • تطوير قدرة الشركة على تحمل المخاطر الإلكترونية ومراقبة التوافق معها. • الإبلاغ عن إجمالي المخاطر الإلكترونية على مستوى الجهة.	• وضع مجموعة مستنيرة من المقاييس الإلكترونية على مستوى الجهة. • مواءمة إطار عمل إدارة المخاطر الإلكترونية مع إطار عمل المخاطر العام. • البحث عن الموهوبين الذين هم على دراية بالمخاطر والأمن الإلكتروني.
الخط الثالث	فريق التدقيق الداخلي الذي يوفر ضمانات لحوكمة المخاطر الإلكترونية الشاملة للشركة.	• تدقيق العناصر الإلكترونية الأساسية، إماتدقيقاً منفصلاً (فيما يخص ضوابط الأصول، مثلاً) أو من خلال عمليات تدقيق ذات صلة بموضوع محدد (على سبيل المثال، إدارة مخاطر الموردين). • تقييم التصميم العام وفاعلية إدارة المخاطر الإلكترونية عبر الخطين الأول للمؤسسة.	• تقديم رؤى لتحسين جودة الضوابط الإلكترونية. • تحديد أفضل نهج لتقييم إطار عمل مخاطر الأمن الإلكتروني بشكل مستقل.

يجب أن يبني قسم المخاطر في الخط الثاني قدراته. وينبغي أن يتم دمج المخاطر الإلكترونية في إطار تحمل المخاطر على مستوى الجهة، حتى تتمكن الإدارة من الموافقة رسمياً على تحملها للمخاطر الإلكترونية. كما يتعين دمج إطار عمل إدارة المخاطر الإلكترونية بشكل كامل في نهج إدارة المخاطر على العموم الأوسع للجهة، وأن ينسجم مع أطر عمل تكنولوجيا المعلومات والمخاطر الأمنية والمخاطر التشغيلية. سيحتاج الخط الثالث (التدقيق الداخلي) إلى تركيز أقوى على الأمن الإلكتروني، والموظفين الجدد (أو القدرات المشتركة)،

ورؤية أكثر استقلالية حول مدى قدرة مجلس الإدارة، والخطين الأول والثاني، على الإشراف على المخاطر الإلكترونية وتقييمها وإدارتها. يتمثل التحدي الرئيسي لجميع الخطوط الثلاثة في إدارة المخاطر الإلكترونية المرتبطة بالغير. تدفع الهيئات التنظيمية نحو المزيد من الرقابة المستمرة والتفصيلية على الغير، لا سيما فيما يتعلق بالأمن الإلكتروني والمرونة وحماية البيانات.

دمج المرونة في الأمن الإلكتروني منذ البداية

بالرغم من التحديات التي يفرضها مشهد المخاطر الإلكترونية المتغير باستمرار، حيث يبدو أن خبرة الجهات التخريبية والتهديدات تتزايد يوماً بعد يوم، تحتاج الحكومة والجهات الحكومية إلى مناقشة فرصة مهمة، وهي دمج المرونة في الأمن الإلكتروني ضمن أساس أي تغيير تنظيمي. وإضافةً إلى ذلك، يجب أن يرتبط دمج المرونة في الأمن الإلكتروني بنشر ممارسة "الثقة عن طريق التصميم"، وهي أمر يصدر من أعلى التسلسل الهرمي إلى أسفله لإدماج الأمن الإلكتروني عند تصميم جميع المنتجات والعمليات والتطبيقات والخدمات أو إعادة تصميمها أو عند النظر في أي شراكة بين القطاعين الحكومي والخاص. ويمكن للإدارة العليا دعم هذا المفهوم وتعزيزه من خلال التحقق الأمني قبل إطلاق المبادرات أو عند بدء العمل على كل مبادرة.

من الضروري أن ندرك أن أجهزة إنترنت الأشياء النموذجية قد تشكل تحديات لمفهوم "الثقة عن طريق التصميم". فقد صُممت هذه التقنيات بشكل عام مع مراعاة السرعة، وقد توفر وصولاً سهلاً للجهات التخريبية التي تقف وراء التهديدات. وبالمثل، فإن العديد من برامج التحول الرقمي لا تتضمن خاصية الأمان حتى يُجرى تنفيذها، وهي عملية تؤدي دائماً إلى إحداث ثغرات أمنية. ومن ثم فإن دعم الإدارة العليا لإدخال المتطلبات الأمنية في وقت مبكر من مرحلتي التصميم ووضع المفاهيم أمر ضروري، إلى جانب دمج الثقة في كل ما يجري تصميمه أو إعادة تصميمه. وقد توجد عادة مقاومة داخلية للتغيير نظراً لوجود تصور عام خاطئ بأن هذا سيؤدي إلى إبطاء الأعمال. فالغرض من هذا الدور المُسند للإدارة العليا هو ضمان تحقيق التعاون منذ المراحل المبكرة، مما يجعله أمراً بالغ الأهمية في نموذج "الثقة عن طريق التصميم".

معادلة المخاطر

يمكِّن دمج الأمن في مرحلة تصميم المبادرات الرئيسية الجهات الحكومية من تخفيف المخاطر، إلا أنه لا يقضي عليها تماماً. لذا قد تحتاج الشركات إلى اتخاذ قرارات صعبة حول أماكن الاستثمار، وهنا يأتي دور التقييم الكمي للمخاطر. إذ من الضروري أن تفهم الأطراف المعنية الرئيسية حجم المخاطر واحتمال حدوثها وتقدير التكلفة المالية للأضرار إن وجدت. ويمكن حساب الحجم المحتمل لخطر معين باستخدام هذه الصيغة: خطر = تهديد (مثل لبرمجيات الخبيثة) × الثغرة الأمنية × التأثير على الجهة (من حيث عملياتها وسمعتها على سبيل المثال). وبينما يوجد العديد من الافتراضات المدمجة في مثل هذه المعادلة، فإن الحكومة والجهات الحكومية تسعى إلى قدر أكبر من التقدير الكمي للموارد المالية من أجل اتخاذ قرارات حوكمة أكثر استنارة حول الإقدام على المخاطر وتحملها.

التقييمات المستقلة

تستخدم العديد من الشركات أطر عمل ومبادئ معروفة للتعامل مع حوكمة الأمن الإلكتروني، إلا أن استخدام جهة خارجية لأغراض التحقق يعد خطوة أساسية في ربط المخاطر بالبرامج والضوابط وربط النتائج بعمليات الجهة. لذا من الضروري أن تعين الحكومة والجهات الحكومية جهة خارجية من أجل تقييم برامجها الأمنية. اختارت بعض الجهات الحكومية إجراء عملية تحقيق ومراقبة بسيطة للغاية مع الرئيس التنفيذي لأمن المعلومات، الأمر الذي استغرق ساعات محدودة. لمزيدٍ من التأكيد، تسعى جهات أخرى إلى تطبيق اختبار مراقبة إضافي لأطر العمل ذات الصلة (منها، على سبيل المثال، المعهد الوطني للمعايير والتكنولوجيا [NIST]). وللحصول على أعلى مستوى من الضمان، يتم طلب رأي طرف خارجي مستقل يستخدم نظام المعهد الأمريكي للمحاسبين القانونيين (AICPA) وضوابط النظام والمؤسسة (SOC) لإطار الأمن الإلكتروني، بما يتيح تقييم برنامج إدارة المخاطر الإلكترونية على مستوى الجهة الحكومية.

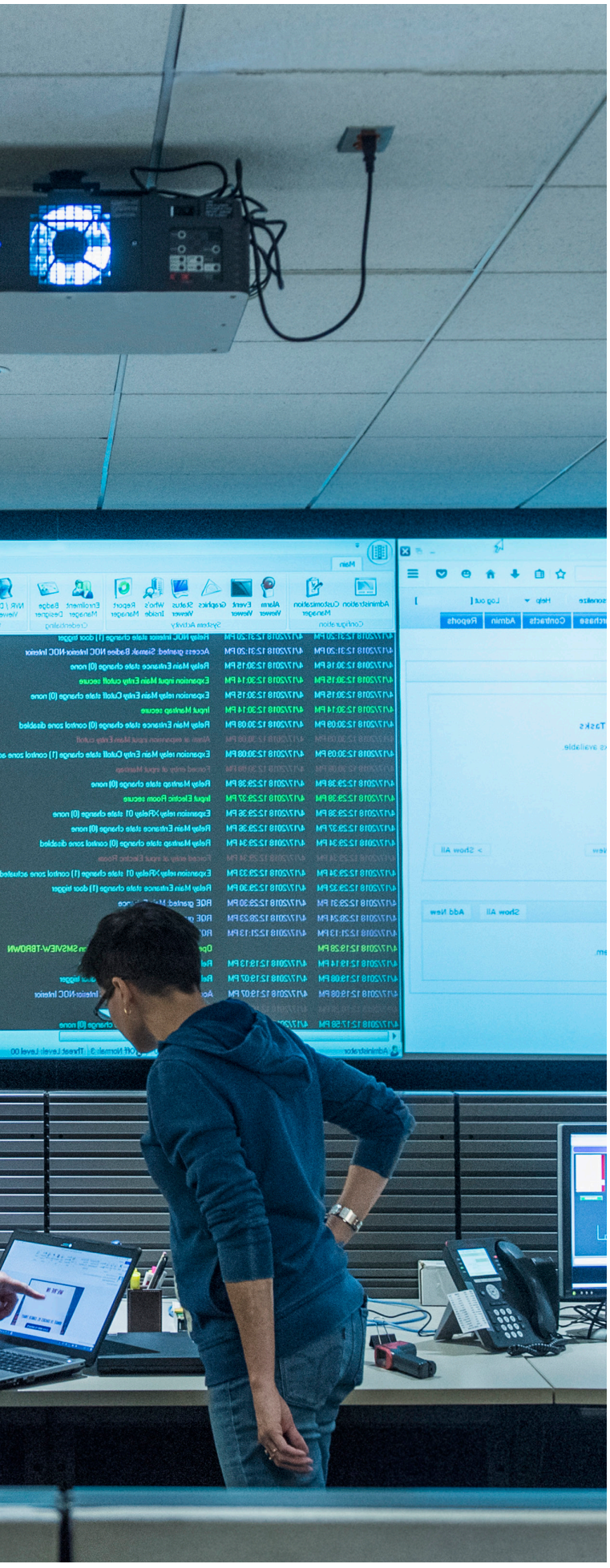
يجب أن نسعى إلى جعل المرونة في الأمن الإلكتروني بداية سلسة لخطوات نحو الحفاظ على الإنجاز المستمر للعمليات في ظل أي أعطال. ويمكن وضع الأساليب

التالية في الاعتبار لتحقيق ذلك:

تقييم ملف المخاطر وتحديد المخاطر والتهديدات ومواطن الضعف الرئيسية

إن تقييم مخاطر المرونة في الأمن الإلكتروني، إلى جانب إسناد الأولوية إلى مدى الخطورة، لبنة البناء الأساسية لأي برنامج للمرونة الإلكترونية. هذه هي الخطوة الأولى نحو تحقيق المرونة في الأمن الإلكتروني ويمكن القيام بها من خلال ما يلي:

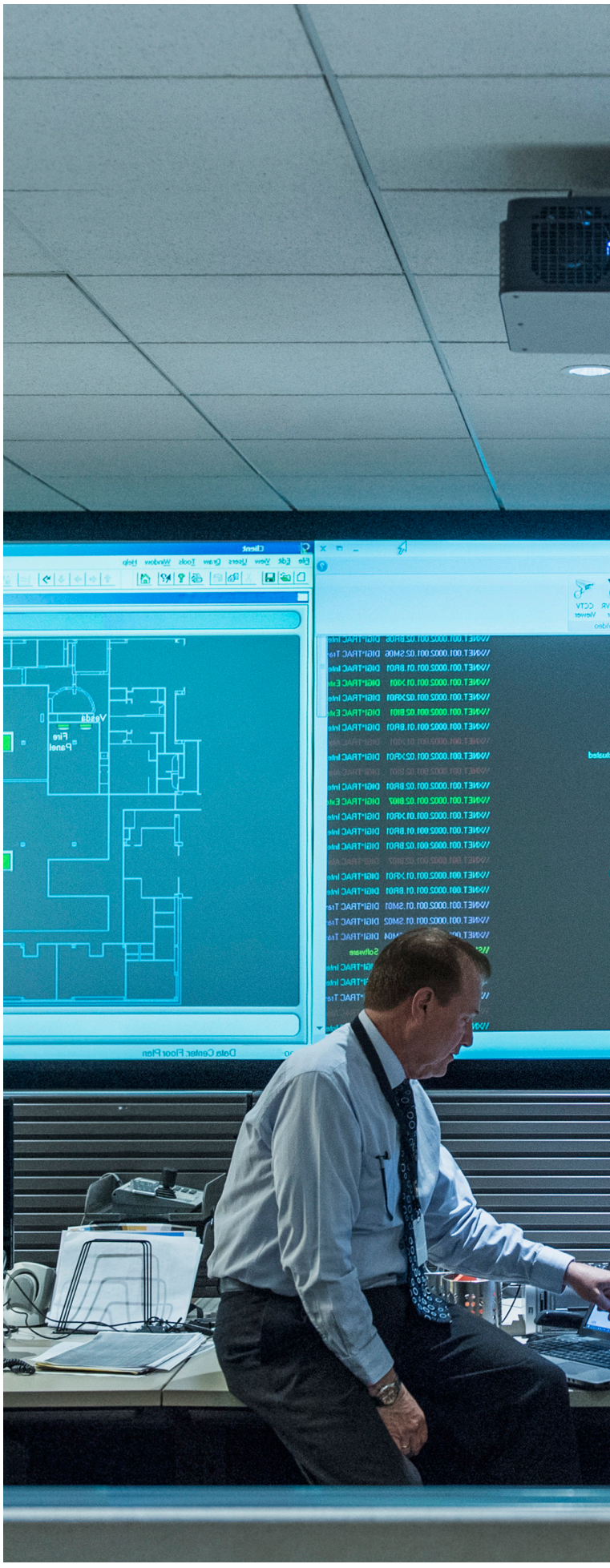
- إعداد عملية تقييم مخاطر فعَّالة: تحديد المخاطر هو دور الخطين الأول والثاني. ما مدى كفاءة الخط الأول في مراعاة المخاطر الإلكترونية ومخاطر المرونة، من وجهة نظرهم؟ ما مدى تقييم الخط الثاني لهذه المخاطر من أجل دحض وجهة نظر الخط الأول على نحو فعَّال وتكملتها.
- سيحتاج تحليل المخاطر من جانب الخطين الأول والثاني إلى إجراء تحديث روتيني؛ نظراً للطبيعة السريعة التطور للمخاطر الإلكترونية.
- وضع ضوابط فعالة: وضع ضوابط في ضوء تقييمات المخاطر يعد أمراً بالغ الأهمية. إذ يجب أن تقلل هذه الضوابط من المخاطر المتبقية في إطار تحمل الشركة للمخاطر بوجه عام من أجل تحقيق المرونة. ويتضمن ذلك الإلمام بكيفية تأثير الاعتماد على الجهات الخارجية على بيئة المراقبة.
- تقديم رأي ذي أولوية على مستوى الجهة الحكومية للعمليات والتدفقات الحرجة: بالنظر إلى الموارد المحدودة ووقت الإدارة والميزانية والأشخاص، يتعين على الشركات حتماً منح الأولوية لأنشطة معينة تتصل بالمرونة وتحديد العمليات والأنظمة التي تتطلب استراتيجية متمايزة. وسيؤدي ذلك على الأرجح إلى وجود وجهات نظر مختلفة داخل كل مؤسسة حول ما يمكن اعتباره أمراً حرجاً. وقد يكون لخط الدفاع الأول للجهة ولجنة إدارة المخاطر والهيئات التنظيمية تعريف مختلف للأمر الحرج. ومن ثم يتعين على الجهات الحكومية إدارة مطالب الأطراف المعنية بشأن تحقيق المرونة.



تحديد الأنظمة وتصميمها وحمايتها

يعد تحديد الأنظمة والأصول الأعلى أهمية (بما في ذلك الأصول العالية القيمة) متطلباً أساسياً لتحقيق المرونة في الأمن الإلكتروني. وبمجرد تحديد الأنظمة الحرجة، يتعين على الجهة الحكومية ما يلي:

- تحديد المنظومة البيئية للأنظمة: يمكن استخدام عدد من التقنيات لتحديد الأصول على نحو مناسب، منها تحليل تأثر العمل (BIA) الذي يمكنه تحديد العناصر والأصول الإلكترونية داخل الجهة نفسها، وتصنيف الأصول الإلكترونية والتقنية بناءً على السرية والسلامة والتوافر (CIA)، وإنشاء ملفات تعريف وسجلات للمخاطر الإلكترونية.
- تقييم وتحسين بنية النظام وتصميمه: يجب أن تتمتع الأنظمة الحرجة بالمرونة والسرعة والصمود بما فيه الكفاية، إذ لا ينبغي تحقيق الأمن الإلكتروني بعد فوات الأوان ويجب علينا دمج الأمن في تصميم بنية النظام. ويتعين على الجهة الحكومية تحديد مجموعة معينة من متطلبات الأمان التي تفرض سلامة الأمن الإلكتروني الرئيسية مثل التجزئة والحد الأدنى من مستوى الوصول والحد من ناقلات التهديد، وما إلى ذلك.
- تقييم ما إذا كانت الأنظمة والأدوات المستخدمة لمراقبة البنية التحتية تتضمن ثغرات أمنية رئيسية أم لا: توظف الجهات الحكومية مجموعة متنامية من الأدوات بغرض تقييم شبكاتها وأنظمتها لاكتشاف التهديدات وتطبيق أدوات التشفير لحماية المعلومات الحساسة، إلا أنه من الضروري أن تتحقق الجهات الحكومية من أن تلك الأدوات، في حد ذاتها، لا تشكل تهديدات أمنية إضافية.



- تقييم تقادم النظام: تعتمد كل جهة حكومية استراتيجيتها الخاصة لإدارة تقادم النظام، مثل السرعة التي تنتقل بها إلى الإصدارات الجديدة من البرمجيات أو الأجهزة، ونهج تصحيح المسار، ودرجة اعتماد الشركة (أو عدم اعتمادها) على الأنظمة التي لم تعد مدعومة من البائع. وبينما قد تكون الاستراتيجية العامة منطقية بالنسبة للجهة الحكومية، فمن الضروري أن تثبت الجهات أنها قد درست بعناية اعتماد استراتيجية متمايزة بالغة الأهمية بالنسبة للأنظمة الحرجة. وكما أظهرت هجمات برامج الفدية الأخيرة على مستوى العالم فإن حالات تعطل الأنظمة يمكن أن تعزى إلى الاعتماد على الإصدارات القديمة وممارسات تصحيح المسار السيئة، فذلك غير مقبول بالنسبة للأنظمة الحرجة.

إدارة الجهات الخارجية الحرجة وحالات الاعتماد الرئيسية الأخرى

تحتاج الجهة الحكومية إلى تقييم حالات الاعتماد على الجهات الخارجية، لا سيما تلك التي تدعم العمليات والأنظمة الحرجة أو تتصل بها. وقد يشمل ذلك إعادة تقييم كيفية تحديد الموردين وحالات الاعتماد الحرجة. يجب تقييم الموردين الحرجين ووضعهم تحت مراقبة أشد مقارنة بغيرهم. يتعين على الجهة الحكومية:

- تقييم مرونة الموردين وممارسات الأمن الإلكتروني: يمكن القيام بذلك قبل تأهيل الموردين، غير أنه سيكون على الأرجح إجراءً متعجلاً فيه ويحتاج إلى إعادة النظر، أو قد فات أوانه. ستحتاج الشركات إلى تحديد مدى سرعة الموردين في إعادة تشغيل أنظمتهم بعد وقوع عطل ما، فضلاً عن تقييم كيفية تقديم المورد الدعم في حال أي تعطل مطول لضمان استمرارية العمل.
- إدارة بنود العقود والالتزامات: تحتاج الجهة الحكومية إلى اعتماد شروط تعاقدية توضح مستوى الأداء إضافةً إلى المخاطر الرئيسية ومؤشرات الأداء التي يتعين على المورد استيفاؤها على وتيرة محددة مسبقاً.
- المراقبة المستمرة: ستحتاج الجهة الحكومية إلى إعادة تقييم نهجها لمراقبة الموردين الحرجين بصفة مستمرة. وفي حال عدم توفر مراقبة آنية، فإن المراقبة شبه الآنية (أي خلال اليوم) ستكون مطلوبة.

المرونة في الأمن الإلكتروني

لا تزال الشركات بحاجة إلى تنفيذ أنشطة الكشف والاستجابة والاستعادة بصورة مستمرة حتى في حال قيامها بأعلى مستويات التخطيط على مستوى العالم. فهي بحاجة إلى التواصل بشكل فعال أثناء الأعطال المحتملة والفعلية. وعند حدوث هجمات إلكترونية، يجب على الجهة الحكومية التحرك بسرعة لاكتشافها والتصدي لها. أما إذا نجحت هذه الهجمات، فستحتاج الشركات إلى تحديد كيفية الرد. وفي سياق المرونة، تشمل محاور التركيز الرئيسية للهيئات التنظيمية والجهات الحكومية ما يلي:

- بناء قدرات الكشف: يعد الكشف عن المشكلات أمراً ضرورياً، فهو بمثابة شريان الحياة لتحقيق المرونة. ومن ثم يجب على الجهة الحكومية وضع برنامج من خلال جمع المعلومات عبر مصادر مختلفة وتحليلها واستخدامها لمواصلة تحسين الوضع الأمني.
- تعزيز قدرات الاستجابة: تعد القدرة على الاستجابة والعمل جزءاً أساسياً من المرونة، ويتحقق ذلك من خلال وجود برنامج استجابة للحوادث. يجب أن يسهل البرنامج الانتقال الفعال من الاستجابة للحوادث إلى إدارة الأزمات. وهو من أفضل الممارسات لاختبار خطة الاستجابة بانتظام من أجل تقييم الفاعلية والحفاظ على براعة الأطراف المعنية الرئيسية في أداء أدوارها ومسؤولياتها.
- تطبيق قدرات الاستعادة والتحسين باستخدام الاختبار: استعادة النظام بعد حدوث عطل أمر مهم، ومن ثم يتعين على الجهة الحكومية تحديد الحوادث الإلكترونية التي تمثل تحدياً خاصاً في مواجهة استعادة النظام عندما تكون الأنظمة معطلة. ويجب مراجعة مواقع الاستعادة بانتظام لضمان قابلية وصول عالية للأنظمة الحرجة. وتعد البيانات، بوصفها جزءاً من عملية الاستعادة، عنصراً مهماً أيضاً، من حيث التحقق من سلامتها وجودتها وضمان عدم التلاعب بها من قبل مهاجم ما أو برمجية ضارة.
- وضع خطط التصعيد والتواصل: يجب على الجهة الحكومية تحديد نهج للتصعيد السريع والفعال خلال أوقات الأعطال. إذ يجب تصعيد الاتصالات عند وقوع مشكلة وتنبيه الأطراف المعنية الرئيسية، مثل خط الدفاع الأول والإدارة العليا والمنظمين والعملاء، إذا لزم الأمر.

القسم الخامس

تطبيق نهج سريع لإدارة المخاطر الإلكترونية وتلبية متطلبات الامتثال

تحتاج الجهات الحكومية إلى اتخاذ خطوات حثيثة لتحديد المخاطر المرتبطة بأعمالها وإدارتها والحماية من الهجمات الإلكترونية من أجل تقليل أي تأثير على العمليات التجارية. إن وضع استراتيجية لإدارة المخاطر الإلكترونية يمكن أن يساهم في اتخاذ قرارات مستنيرة بشأن المخاطر المرتبطة بالعمليات التجارية من منظور داخلي وخارجي.

ولم تعد إدارة المخاطر الإلكترونية أمراً اختيارياً، بل أصبحت ضرورة لمساعدة الجهة الحكومية على تحديد المخاطر الإلكترونية الرئيسية التي يمكن أن تؤثر على أعمالها. ومن ثم فإن الإلمام بالمخاطر وما يرتبط بها من قدرة على تحمل المخاطر يمكن أن يوجه الجهة الحكومية بشأن تخصيص ميزانية وموارد فعالة لتقليل التأثير المحتمل من خلال البدء في وضع ضوابط مناسبة بوصفها تدابير مضادة.

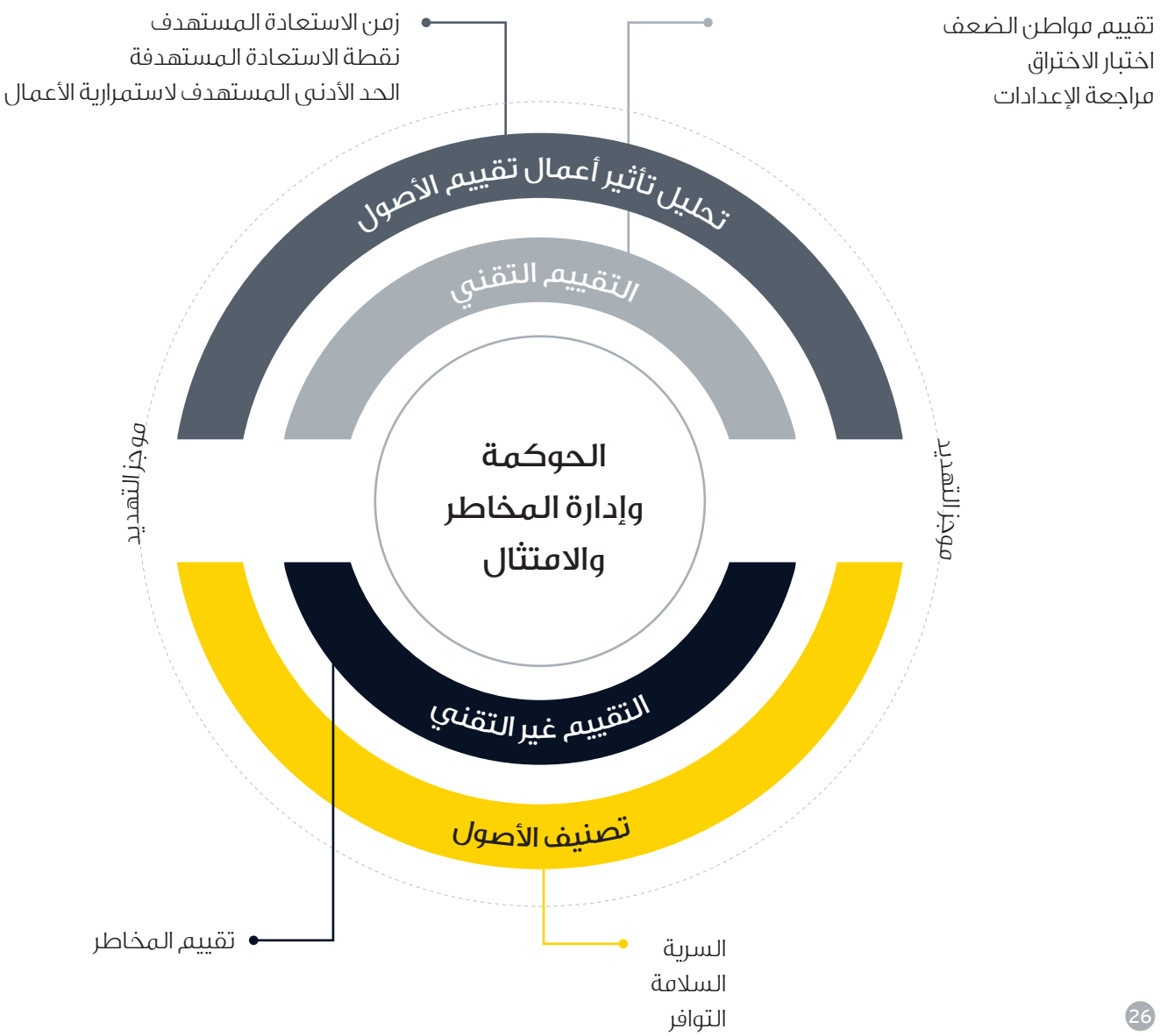
والهدف من عملية إدارة مخاطر الأمن الإلكتروني هو تحديد المخاطر الإلكترونية على أصول معلومات الجهات الحكومية وتقييمها والتخفيف من أثرها ومراقبتها. ويجب أن تكون هذه العملية منهجية وقابلة للتكرار، بحيث يمكن للجهة أن تكون على دراية جيدة بالمخاطر الإلكترونية الأساسية وتتخذ الإجراءات المناسبة لحماية أصولها.

العناصر الرئيسية للمرونة الإلكترونية

يتطلب تحقق المرونة في الأمن الإلكتروني اتباع نهج متكامل للحوكمة والمخاطر والامتثال من خلال مراعاة المخاطر والتهديدات إضافةً إلى قدرات المرونة. ومن أجل الحفاظ على منظومة بيئية مرنة، يعد تمكين وظائف الحوكمة الإلكترونية والمخاطر والامتثال داخل الجهات الحكومية أمراً بالغ الأهمية لتحفيز تلبية متطلبات الأمان الرئيسية عبر مختلف وحدات الأعمال. ويمكن لوظائف الحوكمة الإلكترونية والمخاطر والامتثال أن تستعين بسلسلة من التقييمات من أجل تحديد طبيعة المخاطر والتهديدات ذات الصلة، إضافةً إلى الاستفادة من معلومات التهديدات من المصادر الداخلية والخارجية. يمكننا شرح هذا النهج باستخدام الرسم البياني الموضح أدناه الذي يبدأ بتحديد أهمية الأصول من حيث السرية والسلامة والتوافر (CIA) وكذلك تحليل تأثر العمل (BIA) التقليدي الذي يضع في الاعتبار تأثير الأعطال على سير العمليات.

الشكل 1

المرونة في الأمن الإلكتروني



نهج ثلاثي المحاور لتحديد المخاطر والتهديدات

حددنا نهجاً ثلاثي المحاور لمساعدة الجهات الحكومية على فهم موقفها من المخاطر وتحديد بيئة التهديدات المحيطة بها ومنح الأولوية لحماية الأصول الحرجة، باستخدام سلسلة من التقنيات والتقييمات التي أثبتت جدواها للمؤسسات العاملة في مختلف القطاعات في جميع أنحاء العالم.

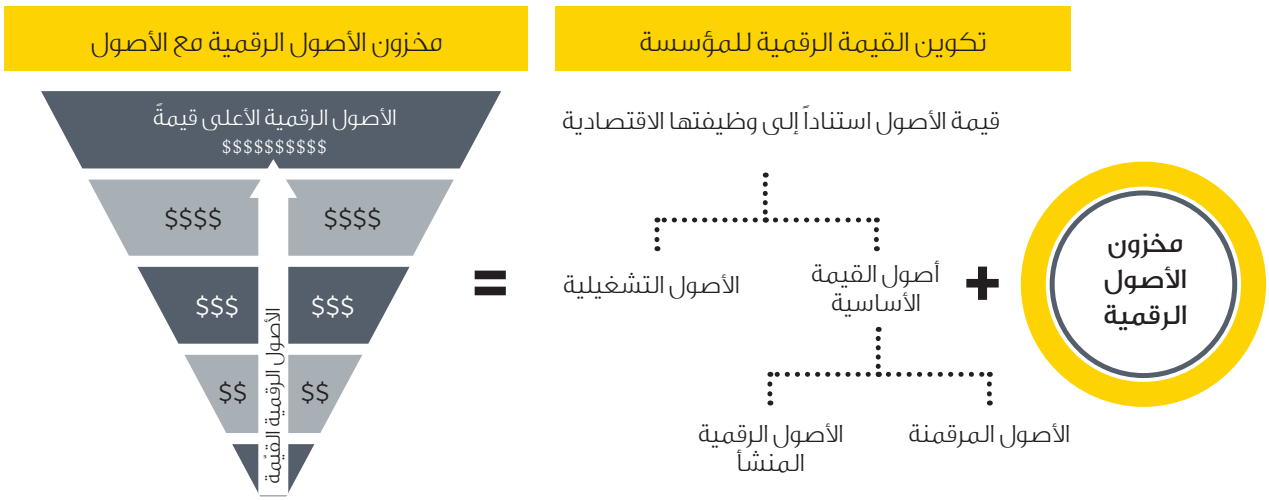
تحديد "الأصول الأعلى قيمةً" لدى الجهات الحكومية

عندما يتعلق الأمر بالأصول الأعلى قيمة لدى أي جهة حكومية، يتعين على الجهة إنفاق كل ما يلزم من أجل، تأمينها مع تفادي تجاوز الحد اللازم للإنفاق من خلال إجراء تقييم شامل باستخدام العملية الموضحة في الشكل 2 أدناه. ويمكن للجهات الحكومية تقييم مرونتها الإلكترونية من خلال أدوات النمذجة الاقتصادية المصممة وفق احتياجات الجهة.

يساعد تطبيق نموذج اقتصادي إلكتروني في تحديد الأصول الأكثر أهمية التي تتطلب الحماية، وتحديد الخسائر الاقتصادية بعد التعرض لهجمات الأمن الإلكتروني. فعلى سبيل المثال، ما الخسارة المقدرة لجهة معينة لو فقدت مليوناً من سجلات عملائها وأصبحت هذه الخسارة علنية؟ من خلال استخدام هذا النموذج، يمكن للجهات الحكومية وضع رسم بياني يحدد كيف ستبدأ القيمة المعرضة للخطر في الانخفاض في ضوء تعزيز الضوابط الدفاعية لمنع الهجمات المرتبطة بتصورات الخسارة الاقتصادية الإلكترونية.

الشكل 2

نهج ثلاثي المحاور لتحديد المخاطر والتهديدات



أ. تصنيف الأصول من حيث السرية والسلامة والتوافر (CIA)

يمكن تحديد أهمية الأصول باستخدام نموذج أمن المعلومات الثلاثي؛ السرية والسلامة والتوافر. ينبغي أن تحظى الجهة الحكومية بإشراف شامل على أصول معلوماتها، ويجب تصنيفها من خلال تقييم كل أصل وفقاً لنموذج السرية والسلامة والتوافر الثلاثي. ويمكن تنفيذ ذلك من خلال تحديد معدل تأثير كل عنصر داخل نموذج السرية والسلامة والتوافر الثلاثي وفقاً لمقياس محدد مسبقاً. على سبيل المثال، يمكن أن يتراوح مقياس معدل التأثير من منخفض إلى مرتفع. ومن ثم يمكن للجهة الحكومية أن تقيس الحد الأقصى للمعدل عبر عناصر نموذج السرية والسلامة والتوافر لكل أصل وتحديد أهمية الأصول وفقاً لذلك.

ومن شأن ذلك أن يساعد الجهات الحكومية على فصل الأصول غير الحرجة عن أنشطة تقييم المخاطر غير الضرورية التي تستغرق وقتاً طويلاً. يدعم هذا النهج وجود مستودع شامل للأصول الأعلى قيمةً يعكس مدى أهميتها وفقاً لنموذج السرية والسلامة والتوافر الثلاثي الذي يركز على تحديد أولوياتها من أجل اتخاذ خطوة تقييم المخاطر.

ب. نهج تكامل الأصول الأعلى قيمةً مع نموذج السرية والسلامة والتوافر

ثمة طريقة أخرى لعرض الأصول الأعلى قيمةً، وهي النظر إلى العمليات التجارية بوصفها أصولاً يمكن أن تتعرض للمخاطر الإلكترونية. ومن ثم تصبح إجراءات العمل عاملاً أساسياً يجب على الجهات الحكومية مراعاته عند تحديد الأصول، على نحو يتوافق مع إجراء تحليل تأثر العمل (BIA).

ويمكن للجهة الحكومية الارتقاء بمستودع أصولها الأعلى قيمةً من خلال دمج أصولها الحرجة مع إجراءات العمل الأشد حرجاً في الجهة. ومن ثم فإن وجود نهج متكامل يساعد في بناء المرونة والجهود الإلكترونية جنباً إلى جنب من أجل تحقيق رقابة صارمة على المخاطر الإلكترونية داخل الجهة الحكومية.

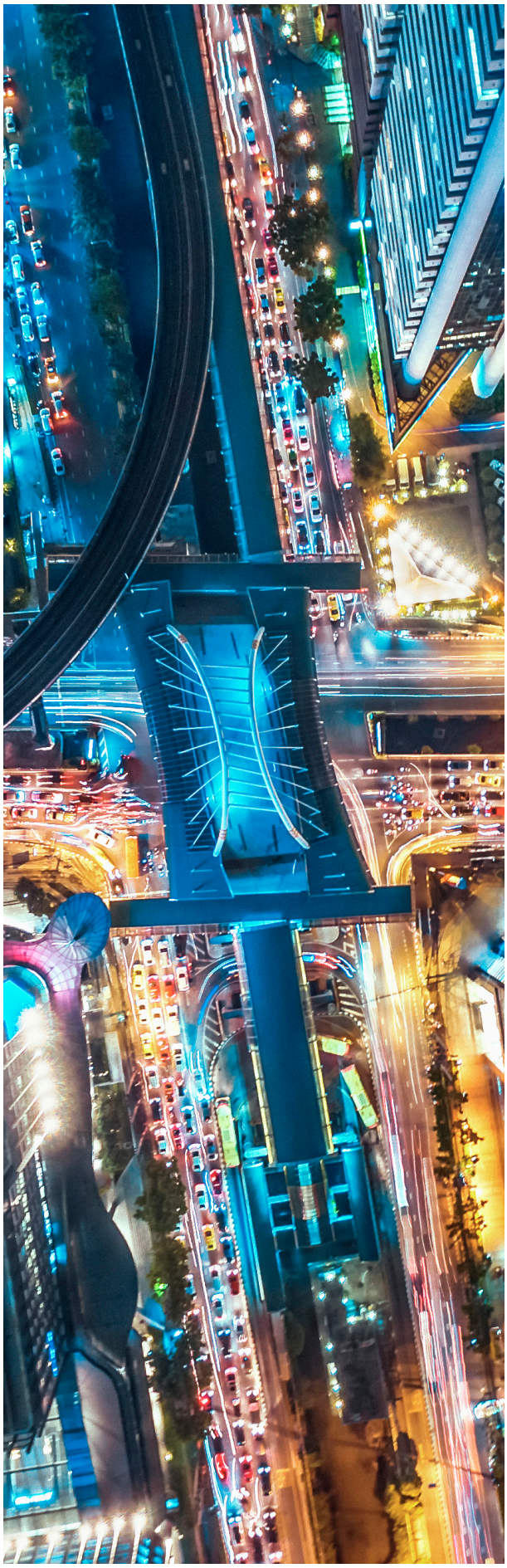
وإضافةً إلى ذلك، يضيف دمج إجراءات الأعمال مزية كبيرة إلى مستودع الأصول الأعلى قيمةً تمكّن الجهات الحكومية من ربط زمن الاستعادة المستهدف (RTO) ونقطة الاستعادة المستهدفة (RPO) بكفاءة في كل عملية تجارية. ويمكن للجهات الحكومية أن تشرف على تأثير الأعمال ومضاعفاتها في حال الاستغلال الناجح للأوضاع، مما يساعد في تخفيف أثر المخاطر على نحو مستنير واستباقي.

تقييم مخاطر الأمن الإلكتروني

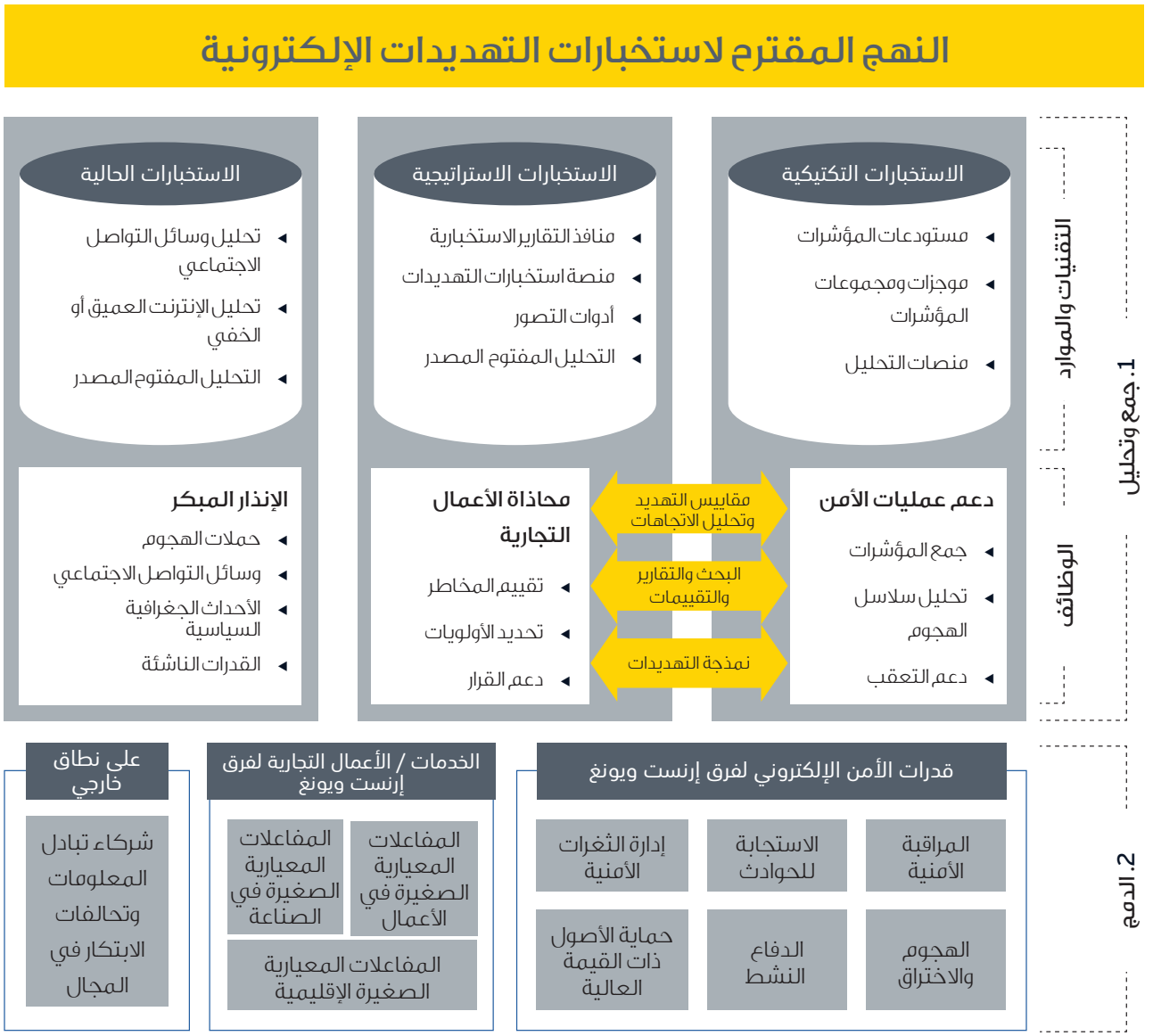
أ. الاستفادة من المعلومات الخاصة بالتهديدات وملخصاتها

من الضروري الاستثمار في استخبارات التهديدات الإلكترونية (CTI) لفهم وضع الجهة الحكومية من حيث المخاطر والأساليب والتقنيات والإجراءات المحتملة (TTPs) وتقييم الطريقة التي يدبر بها منفذو التهديدات الهجمات ويديرونها. وغالباً ما ترتبط استخبارات التهديدات الإلكترونية ارتباطاً وثيقاً بمطاردة التهديدات الإلكترونية (CTH) وتوفر رؤية للمخاطر المناسبة التي تسمح للجهات الحكومية بتحديد مجموعة قدرات المرونة المطلوبة لديها. وتعد مطاردة التهديدات الإلكترونية من أنشطة الدفاع الإلكتروني الفعَّالة. وهي عبارة عن عملية بحث استباقي ومتكرر عبر الشبكات لاكتشاف التهديدات المتقدمة التي تتهرب من الحلول الأمنية الحالية وعزلها.

تركز استخبارات التهديدات الإلكترونية على تحديد وتحليل الدوافع والأساليب والقدرات والأدوات الخاصة بالخصوم الذين قد يسعون لاستهداف إحدى الجهات عن طريق دمج التحليل الخارجي بالبيانات التي كانت مجزأة سابقاً داخل الجهة. وبينما قد تختار بعض الجهات الحكومية تعريف استخبارات التهديدات الإلكترونية بوصفها مكوناً أو خدمةً تعتمد على المدخلات، فمن الضروري ملاحظة أن دورة حياة الاستخبارات القائمة على العمليات ضمن إطار عمل تشغيلي تعد ضرورية لتقديم نتائج فعَّالة. ووفقاً لذلك، يلزم وجود برنامج شامل لاستخبارات التهديدات الإلكترونية يتألف من عمليات لجمع المعلومات الاستخبارية التكتيكية والاستراتيجية وإنتاجها ونشرها إلى جانب التعزيز المستمر لتحديثات التوعية بالأوضاع في الوقت المناسب (والتي تُعرف أيضاً باسم "الاستخبارات الحالية"). حيث يساعد ذلك في تحديد الخصم المعني، وطريقة وأسباب هجومه المحتمل على الجهة، والإجراءات التي يمكن أن يتخذها بعد التسوية الأوَّلية، وأين يمكنه التواجد داخل الجهة، وطريقة اكتشاف الهجوم أو الرد عليه.



الشكل 3



ينبغي دمج استخبارات التهديدات الإلكترونية التي جرى جمعها وإنتاجها من خلال عمليات مصممة لدعم صناع القرار والعمليات الأمنية والمسؤولين عن المرونة. ويجب تصميم عمليات الإدخال ونواتج برنامج استخبارات التهديدات الإلكترونية بهدف تحسين الوعي بالتهديدات الإلكترونية في الجهة الحكومية بأكملها عبر مختلف المستويات. وترى فرق عمل شركة إرنست ويونغ أنه يمكن تحقيق ذلك عندما يُنظر إلى استخبارات التهديدات الإلكترونية من خلال عدسة مكونات الاستخبارات "التكتيكية" و"الاستراتيجية" و"الحالية" وتسليمها إلى الأطراف المعنية بغرض تحديد خطط تحقيق المرونة في الأمن الإلكتروني واختبار آليات الاستجابة للأزمات الإلكترونية.

ب. تحديد المخاطر الإلكترونية الداخلية والخارجية

الهدف من تحديد المخاطر هو اتخاذ قرار حول ما يمكن أن يتسبب في وقوع خسارة محتملة، واكتساب معرفة متعمقة حول طريقة حدوث الخسارة ومكان وقوعها والأسباب التي قد تؤدي إليها. ومن ثم يجب على الجهات الحكومية العمل على تحديد وتقييم المخاطر الإلكترونية الداخلية والخارجية المحتملة بوصفها خطوةً أوَّليةً للسيطرة على المخاطر. ويمكن التعامل مع تحديد المخاطر الإلكترونية من خلال نهج قائم على التصورات المحتملة أو نهج قائم على التصنيف إلى فئات من أجل الإلمام بالثغرات الأمنية ذات الصلة.

ج. تحليل المخاطر الإلكترونية وتقييمها

عندما يتعلق الأمر بتقييم المخاطر الإلكترونية، يجب على الجهات الحكومية مراعاة التأثير الذي يمكن أن تسببه المخاطر الإلكترونية المحتملة وإمكانية وقوعها مما يؤدي إلى الإلمام بالمعلومات المرتبطة بتصنيف المخاطر الكامنة إلى مخاطر حرجة أو عالية أو متوسطة أو منخفضة الشدة. (التأثير × الاحتمال = المخاطر الكامنة).

ومن ثم يجب على الجهات الحكومية مواصلة تحليل تصنيف المخاطر الكامنة من خلال تحديد وتقييم الضوابط الأمنية المطبقة حالياً ومدى فاعليتها من أجل الكشف عن نقاط الضعف والثغرات الأمنية، و لفهم التأثير المنخفض وإمكانية الاستغلال الناجح للأوضاع، مما يؤدي إلى توفر معلومات حول المخاطر المتبقية، والتي تعد تصنيفاً نهائياً لمخاطر إلكترونية معينة.

ويمكن استخدام التقييمات الفنية في إطار تقييم المخاطر من أجل التحقق من المخاطر المحتملة على عناصر التكنولوجيا. وفي الغالب، يجري تقييم الثغرات الأمنية واختبار الاختراق (VAPT) ومراجعة الإعدادات التي تتحقق من تشديد الضوابط لاستكمال عملية تقييم المخاطر المعتادة. إلا أنه بناءً على المخاطر التي جرى تحديدها ومدى تعقيد عملية التطبيق، يوصى باستخدام تقنيات مراجعة إضافية مثل مراجعات الدمج وتحليل الشفرات الديناميكية وغيرها لضمان اكتشاف جميع المخاطر المحتملة وتقييمها.

أنواع التقييمات الفنية التي يمكن استخدامها جنباً إلى جنب مع تقييم المخاطر لاكتشاف نقاط الضعف والثغرات الأمنية الفنية بدقة

- تقييم الثغرات الأمنية واختبار الاختراق (VAPT): يعد هذا التقييم من التقييمات الفنية الأكثر استخداماً، حيث يستهدف البنية التحتية الفنية للجهة الحكومية بالكامل استناداً إلى نطاق التقييم.
- مراجعة الإعدادات: تعد مراجعة الإعدادات جانباً أساسياً من جوانب تحصين النظام، ويتضمن ذلك مراجعة آمنة للإعدادات الأساسية لعنصر معين داخل النظام.
- اختبار الاختراق أو اختبار اختراق الفريق الأحمر: يعد هذا الاختبار تدريباً عملياً على الهجمات الناجحة بغرض تحسين دفاعات الأمن الإلكتروني للجهة الحكومية والتأكد من الاستعداد لحمايتها من الهجمات الحقيقية ضمن بيئة تشغيلية.

إعداد خطط للتعامل مع المخاطر وعملية القبول

يجب على الجهات الحكومية وضع إدارة مخاطر الأمن الإلكتروني ومعالجتها في مقدمة أولوياتها،بالنظر إلى البيئة التقنية المتغيرة التي تزيد المخاطر الإلكترونية غير المدارة. ينبغي تركيز الجهود على معالجة المخاطر الإلكترونية الحرجة بشكل فعال وسريع حيثما لزم الأمر، تجنباً للعواقب غير المرغوب فيها.

وبعد الحصول على نتائج منظمة لتقييم المخاطر الإلكترونية، يمكن للجهات الحكومية تحديد المخاطر الأكثر حرجاً بناءً على تصنيف المخاطر المتبقية واتخاذ قرار مستنير على ضوئها بشأن كيفية المضي قدماً في معالجة المخاطر. وإذا كان خيار العلاج المقترح يميل إلى التخفيف، فإنه يجب على الجهة وضع خطة علاج فعَّالة يتم تحليلها والتحقق منها لمعالجة المخاطر الإلكترونية المحددة وحماية الجهة وفق نموذج السرية والسلامة والتوافر (CIA).

أما إذا كان خيار العلاج المقترح يشير إلى قبول المخاطر أو نقلها أو تفاديها، يجب على الجهة الحكومية وضع عملية إدارية لكل خيار علاج مقترح للتأكد من الإلمام بالمخاطر وإدارتها ومعالجتها على نحو جيد وفقاً للعملية التنظيمية المعتمدة.

أتمتة لوحات المعلومات واستخدامها لرصد المخاطر بصورة شبه لحظية

يجب على الجهات الحكومية التفكير في استخدام لوحة معلومات آلية لإدارة المخاطر تتكامل مع نتائج تقييم المخاطر. يمكن أن يساعد ذلك في الإشارة إلى تصنيفات المخاطر والمعلومات المرتبطة بها وعرضها بدقة على لوحة معلومات تنفيذية شاملة. تتمتع الجهات الحكومية التي تعمم هذا المستوى من العناصر التمكينية الناضجة بقدر إضافي من التبصر والتحكم بمخاطرها الإلكترونية، حيث إنها تتيح الحصول على رؤية شاملة لفهم المخاطر التي تشكل أكبر تهديد لعمليات الجهة وأعمالها، وإدارتها وفقاً لذلك.

يساعد استخدام لوحة معلومات إدارة المخاطر في تحسين عملية مراقبة المخاطر من خلال تقديم عروض مرئية لمراجع إحصائية مركزة لنتائج تقييم المخاطر. يشكل هذا بصورة أساسية مراقبة تصنيفات المخاطر والتقدم المحرز في معالجة المخاطر المرتبطة بها. إضافة إلى ذلك، يمكن لمالكي الأصول تصور وضع المخاطر في لوحة معلومات موحدة، مما يوفر طريقة سهلة وفعَّالة لتحليل عواقب المخاطر الإجمالية ويمكن أن يساعد في اتخاذ الإجراءات التصحيحية اللازمة.

توضح لوحة معلومات إدارة المخاطر حالة مؤشرات الأداء الرئيسية للمخاطر في الجهة الحكومية (KPI) وتمكن موظفي الأمن الإلكتروني من مراقبة التقدم المحرز في أنشطة معالجة المخاطر، وتوضح لوحة المعلومات المكونات التالية (على سبيل المثال لا الحصر):

- عدد التهديدات المحددة
- النسبة المئوية للمخاطر المحددة عبر مقياس التصنيف
- متوسط المخاطر لكل مالك
- متوسط المخاطر المعالجة

تساعد أتمتة لوحة معلومات إدارة المخاطر في توصيل معلومات المخاطر بصورة أفضل بين الجهات المعنية، إذ توفر تقنيات التصور نظرة عامة سريعة على اتجاهات المخاطر الرئيسية وتسمح لموظفي الأمن الإلكتروني بإدارة المخاطر المحددة وتحديد أولوياتها.

تحقيق الامتثال من خلال إدارة المخاطر:

ينبغي أن يكون برنامج إدارة مخاطر الأمن الإلكتروني متوائماً ومتوافقاً مع المعايير الوطنية والدولية المعمول بها. ينبغي اعتبار اللوائح معياراً لأداء أنشطة تقييم المخاطر. تلتزم الجهات الحكومية بتحديد متطلبات الامتثال اللازمة استناداً إلى تشريع الجهة المعمول به والمهام الخاصة بالقطاع.

عدم الامتثال للمهام المنظمة يعرّض نسبياً الجهات الحكومية إلى المخاطر والتهديدات مثل العقوبات المالية والإضرار بالسمعة.

يمكن للمؤسسات التي تتبع نظام إدارة مخاطر الأمن الإلكتروني وفقاً لمتطلبات الامتثال أن تحدد بسهولة الضوابط المقررة وتقيّم المخاطر الناشئة عن التقصير في الضوابط المقررة أو عدم تنفيذها على نحو فعال. وبذلك، يصبح بمقدور المؤسسات مراقبة وتتبع حالة الامتثال لكل ضابط من الضوابط نتيجةً لمخرجات تقييم المخاطر. كما يصبح بالإمكان الاستفادة من وجود خطة علاجية للمخاطر لترسيخ خطة الامتثال العلاجية وفقاً لذلك.

يمكن للتعاون المستَثْمَر بين إدارة المخاطر الإلكترونية وإدارة الامتثال أن يقترح منهجية موحدة لتحقيق كلا الجانبين مع تقليل الوقت والجهد المخصصين لكل مهمة على حدة.

القسم السادس

إدارة استمرارية الأعمال وتعريف الاستجابة واستراتيجيات التعافي

مع التطور المستمر في عالم الرقمنة، يعتمد المشهد الاقتصادي الحالي العالمي على الحلول القائمة على التقنية والعمليات الرقمية أو الآلية. معظم هذه الأشياء مفتوحة على العالم بأكمله عبر الإنترنت. وهذا ينشئ مساحة من التهديد الإلكتروني الذي يفرض على الجهات الخدمية والحكومية الاستثمار في إدارتها والتوجه نحو حماية خدماتها. لذا ينبغي دمج مفاهيم المرونة في الأمن الإلكتروني في أنشطة استمرارية الأعمال المؤسسية لضمان توافر الخدمات الأساسية وتقليل تأثير الاضطراب على الخدمات المقدمة للمنتفعين.

تتمثل إحدى أبرز منهجيات التعامل مع المرونة في الأمن الإلكتروني على صعيد استمرارية الأعمال في استخدام نهج المخاطر على مستوى المؤسسة. تسعى هذه المنهجية إلى دمج أنشطة إدارة مخاطر استمرارية الأعمال مع أنشطة إدارة المخاطر المنفذة على المستوى التنظيمي، بما في ذلك المجال الإلكتروني.

ومن جهة أخرى، فعند تحديد المخاطر الإلكترونية، ينبغي مراعاة مخاطر استمرارية الأعمال من ناحية:

- الجانب التشغيلي مثل سلامة ورفاهية و توافر الموظفين المسؤولين عن إدارة وأداء الأنشطة اليومية الإلكترونية. قد تنتقص استمرارية أنشطة إدارة ومتابعة الأمن الإلكتروني مثل الأعطال من وضوح الرؤية في مساحة التهديدات والانتهاكات المحتملة للمؤسسة.
- منظور التأثير المتتالي والمترابط. وخير مثال على ذلك انقطاع الكهرباء الذي يُنظر إليه بوصفه اضطراباً بسيطاً غير متعمد، وقد يكون في الواقع خللاً متعمداً ضمن هجوم إلكتروني متقدم للتغلب على ضوابط الأمن المادي، والضوابط الموجودة في المكان مثل كاميرات المراقبة.

يتطلب تقييم ملف مخاطر الجهة الحكومية تعريف الخطط العلاجية للمخاطر، حيث يشكل هذا اللبنة الأساسية في تعريف استراتيجيات وحلول المرونة المناسبة. وفر المجال رقم 17 من معيار الآيزو 2013:27001 توجيهاً مناسباً للجهات الحكومية الراغبة في تبنّي الاستمرارية في قدراتها الإلكترونية. ينبغي أن تغطي هذه الاستراتيجيات والحلول عدة دعائم أساسية تشمل الناس والتقنية والموقع والسجلات الحيوية والتقنيات التشغيلية والمتطلبات التشغيلية. ويتعين اعتبار ملف المخاطر الإلكترونية جزءاً لا يتجزأ من هذه الأنشطة.

نقطة التقاء أخرى بين المرونة في الأمن الإلكتروني واستمرارية الأعمال هي خطط الاستجابة والتعافي. ينبغي أن تحدد هذه الخطة خطوات العمل نحو استئناف العمليات ضمن فترة زمنية مستهدفة للتعافي.

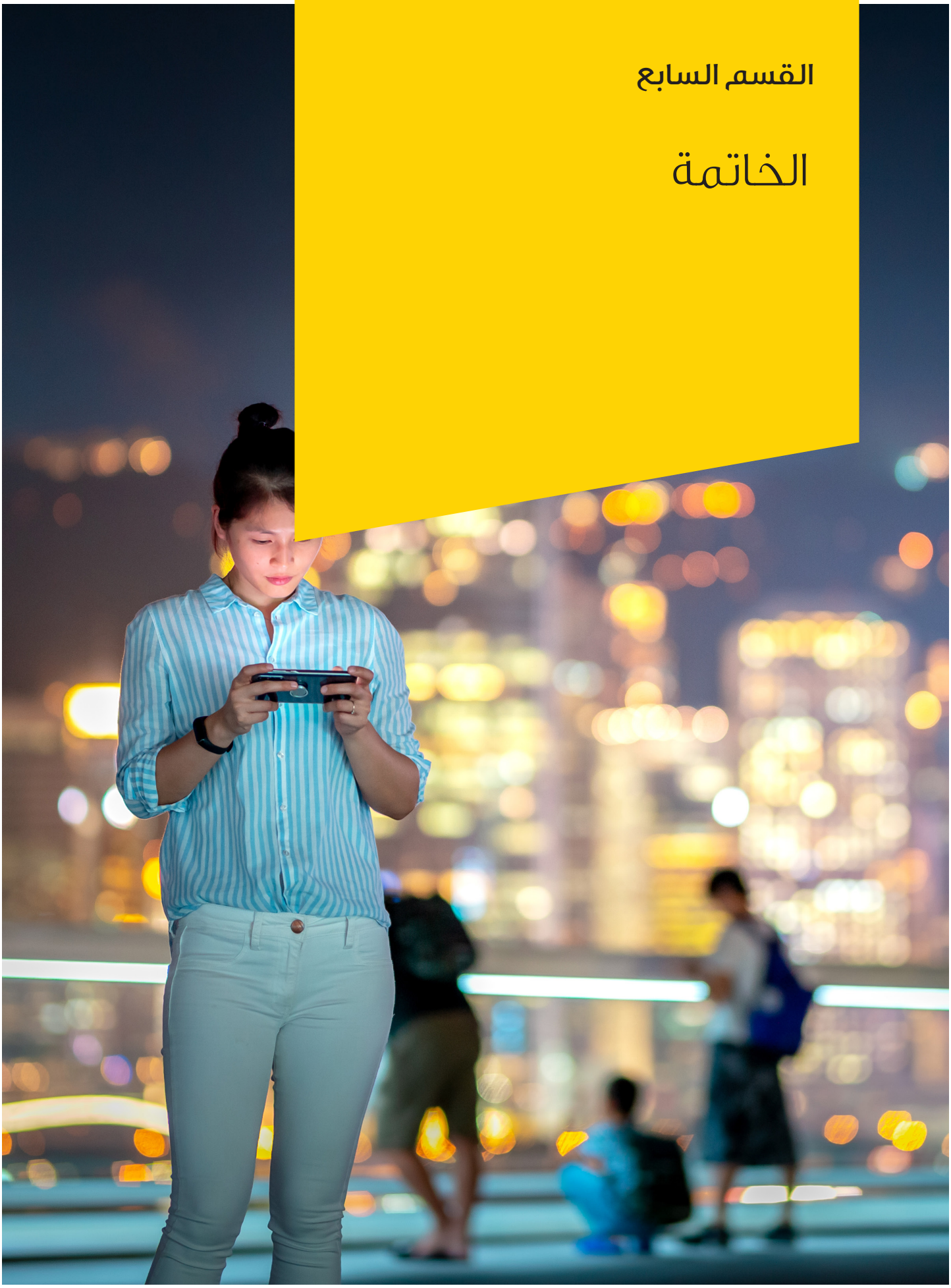
ومن المهم للغاية تقييم الخطة الموضوعة لضمان السريان والفاعلية في المواقف المعاكسة. يمكن للجهات الحكومية تنفيذ عمليات محاكاة أمن إلكتروني لاختبار الخطة ولقياس مدى وعي الأطراف المعنية الرئيسية بمسؤوليتها خلال الأعطال أو الأزمات أو لبناء الخبرات.

وأخيراً، فإن للتكيف مع الأوضاع بعد وقوع عطل، سواء كان إلكترونياً أو غير إلكتروني، أهمية بالغة، بالنظر إلى قدرته على جعل الوضع اعتيادياً في الجهة. فعلى سبيل المثال، طبقت معظم المؤسسات مفهوم العمل عن بُعد لمعالجة المخاطر المرتبطة بالاستمرارية خلال جائحة كوفيد-19. وقد نظرت العديد من المؤسسات إلى هذا الإجراء بوصفه حلاً أكثر فاعلية من ناحية التكلفة مقارنةً باستخدام موقع بديل للعمل أو حتى الموقع الرئيسي، مما أدى إلى ظهور نماذج تشغيل جديدة. وبذلك، أصبح العمل الافتراضي الوضع الاعتيادي الجديد ، الأمر الذي يستلزم تنفيذ ضوابط إلكترونية محكمة لضمان المرونة.

وفي النهاية، فإن المرونة هي الانضباط التنظيمي والسرعة في تطوير القدرات والتعزيز الدائم لها بهدف ضمان التسليم المستمر للخدمات الرئيسية بما في ذلك الأمن الإلكتروني. ينبغي أن تتبنَّى الجهات الحكومية مفهوم الإلمام بالحالة والتعاون بما يسهم في ترسيخ المرونة في ثقافتها.

القسم السابع

الخاتمة



تعمل التقنيات الجديدة على تسريع وتيرة التغير الرقمي والاستخدام الواسع النطاق للأتمتة وتحليلات البيانات والسحابة الإلكترونية. يتزايد اهتمام الحكومة والجهات الحكومية بقدراتها فيما يتعلق بالمرونة وتتطلع إلى توفير نهج أكثر أماناً وتأميناً وبأسعار معقولة لتأمين أنظمتها وبياناتها. فقد يكون الانتهاك القادم من مورد أو طرف ثالث من أكبر المخاطر التي تواجهها.

في ظل التركيز على المعلومات، والاتصالات، والتكنولوجيا (ICT) وخدمات الإدارات الأخرى ومنتجاتها، تتطلب الحكومة والجهات الحكومية فهماً أفضل للمخاطر التي يمكن أن يشكلها المورد بالنسبة للجهة، والأصول المهمة التي قد تكون مستهدفة، والمخاطر الإلكترونية التي قد تنجم عن الأشخاص والعمليات والتقنيات. من خلال فهم المخاطر المحتملة، ستكون القيادة أو الإدارة العليا قادرة على اتخاذ قرارات مستنيرة بشأن المخاطر فيما يتعلق بإجراءات الحد من وطأة المخاطر المحتملة.

لو سلّمنا بأن التعرض لشكل من أشكال الهجوم الإلكتروني أمر لا مفر منه، فستزداد أهمية تطبيق الجهة الحكومية لأنظمة واستراتيجيات تعمل على إعادة العمل كالمعتاد بأسرع طريقة ممكنة، والتعلم مما حدث، والتكيف وإعادة تصميم الجهة الحكومية لتحسين المرونة في الأمن الإلكتروني مستقبلاً. ومن الضروري أن يكون لدى الحكومة والجهات الحكومية برنامج مركزي للاستجابة للاختراق الإلكتروني على مستوى كل جهة (CBRP) أو خطة لإدارة الأزمات الإلكترونية تجمع بين مجموعة واسعة من المعنيين الذين يجب أن يتعاونوا لمعالجة الخرق. ويجب أن يقود هذا البرنامج شخص ذو خبرة في التكنولوجيا وقدرة على إدارة الاستجابة التشغيلية والتكتيكية اليومية. كما يجب أن يتمتع هذا القائد بخبرة متعمقة في القانون والامتثال، إذ يمكن لأي خرق إلكتروني أن يؤدي إلى مشكلاتٍ قانونية وتنظيمية معقدة ذات تبعات مالية.

عندما يتعلق الأمر بحوكمة الأمن الإلكتروني، فإن من أهم الأشياء التي يمكن للجهات الحكومية القيام بها هو تحديد المسار المناسب لتنفيذ ذلك والتوافق مع الإدارة بشأن التحمل المناسب للمخاطر المتعلقة بالأمن الإلكتروني. ويمكن للإدارة العليا للجهات الحكومية إرسال هذه الرسالة جزئياً من خلال حوكمتها والتركيز على الأمن الإلكتروني. فمن الضروري أن تأخذ الإدارة العليا الأسئلة التالية في اعتبارها:

- كم من الوقت يقضيه المعنيون الرئيسيون في تعزيز الأمن الإلكتروني على مدار العام؟
- هل يوضع الأمن الإلكتروني على جدول أعمال الاجتماعات مرة واحدة في السنة أم أنه جزء من معظم الاجتماعات؟

تتحمل الإدارة العليا بشكل أساسي المسؤولية عن الاستراتيجية وإدارة المخاطر، ومن المستحيل فعلياً إجراء هذه المحادثات دون مناقشة شاملة حول التكنولوجيا والأمن. والإدارة العليا التي تركز بصورة مناسبة على الأمن الإلكتروني هي تلك التي تواظب على إدراج هذا الموضوع في مناقشات منتظمة حول الاستراتيجية والمخاطر، وتعطي الأولوية للتعليم الذاتي وتطلب المشورة الخارجية لتعزيز الكفاءة الإلكترونية للجهة، كما تجري مناقشات غير منقحة مع كبير مسؤولي أمن المعلومات (CISO) في الجلسات التنفيذية وترسل باستمرار رسالة واضحة إلى الإدارة مفادها أن إعطاء الأولوية للأمن الإلكتروني جزء لا يتجزأ من الجهة الحكومية.

أمر مهم آخر لتهيئة الجو المناسب هو التأكيد على أن المخاطر الإلكترونية ليست مجرد مشكلة تتعلق بتكنولوجيا المعلومات ولكنها مشكلة على مستوى الجهة الحكومية تشمل جميع الأقسام والوظائف. وبالتالي، تحتاج الإدارة بخلاف مهمة الأمن، إلى أن تكون ضليعة بشأن الضوابط والإجراءات التي تحمي عملياتها، وكيفية تدريب الموظفين واختبارهم بدءاً من الإدارة وصولاً إلى الخط الأمامي، وماهية البروتوكولات التي يجب اتباعها في حال وقوع اختراق أو حادثة إلكترونية.

من خلال اتباع نهج فعَّال للرقابة والحوكمة الإلكترونية، تلعب الإدارة العليا دوراً مهماً في تشجيع أصحاب الاختصاصات والأقسام على تولي مسؤولية أكبر تجاه المخاطر الإلكترونية، ويتعين عليها فهم ما إذا كانت مسؤولية الأمن الإلكتروني مشارَكة على امتداد الجهة الحكومية وكيف تتم مشاركتها.

دمج الأمن الإلكتروني في محادثات الإدارة العليا الشاملة مع كبار المدراء التنفيذيين وقادة الأقسام يوضح أن الأمن الإلكتروني جزءٌ لا يتجزأ من العمليات في جميع أنحاء الجهة، وأن القادة مسؤولون عن دورهم في دعم البنية التحتية للأمن الإلكتروني. إن إعطاء الأمن الإلكتروني الأهمية نفسها التي تحظى بها الشؤون المالية والقانونية في القرارات الحاسمة، يسلط الضوء على كونه مسألة حاسمة في نطاق العمل.

دعوة للعمل

قد يكون إنشاء نهج شامل قائم على الأعمال لمكافحة الهجمات الإلكترونية أمراً مربكاً حينما تكون الجهة الحكومية تعاني بالفعل اضطراباً على العديد من الجبهات المختلفة. ومع ذلك، يجب أن يكون الأمن الإلكتروني من أولويات العمل الأساسية ويُمنح الأولوية من قِبل الحكومات الحديثة والجهات الحكومية. فيما يلي أهم 10 أمور يجب على الإدارة أخذها في الاعتبار أثناء تنفيذ خطط المرونة في الأمن الإلكتروني:

1. دمج الأمن الإلكتروني في استراتيجية المواهب واستحداث منصب كبير مسؤولي أمن المعلومات بما يتناسب مع غرض الجهة الحكومية. ويجب أن يتمتع كبير مسؤولي أمن المعلومات (CISO) بالمرونة لتحديد هيكل تنظيمي يأخذ مجموعة واسعة من العوامل في الاعتبار ويضع المرونة في مقدمة مخططات الأولويات الخاصة به.

2. تحديد مسؤوليات الأمن الإلكتروني لدى الجهة الحكومية بوضوح وإنشاء مصفوفة توزيع المسؤوليات (RACI matrices) التي تشرح مسؤوليات جميع المعنيين بالحفاظ على المرونة الإلكترونية خلال وقوع أي حادث والمساءلة التي يخضعون لها وأدوارهم التي تم التشاور بشأنها والإبلاغ بها.

3. وضع الأمن الإلكتروني في طليعة استراتيجية عمل متعددة المهام. إذ يجب ألا يُنظر إليه على أنه مشكلة تتعلق بتكنولوجيا المعلومات وينبغي النظر إلى وظائف الأمن الإلكتروني على أنها عامل تمكين من جانب الوظائف الداعمة. ويتعين تعميم خطط المرونة على جميع المعنيين وإبلاغهم بها.

4. التأكد من أن الأمن الإلكتروني جوهر الابتكار الرقمي وعامل مساعد له وليس عائقاً أمامه. فالتحدث عن تضمين مفهوم "الثقة عن طريق التصميم" أسهل من تنفيذه. لذا فإنه من الضروري للإدارة التنفيذية أن توفر الدعم للجوانب والمتطلبات الأمنية مع التعريف بأهمية إدارة المخاطر الإلكترونية والمرونة في الأمن الإلكتروني عبر جميع وحدات الأعمال.

5. فهم كيفية تأثير القواعد التنظيمية على العمليات، والعمل مع الهيئات التنظيمية لإرساء قدرات المرونة في الأمن الإلكتروني التي تعالج المتطلبات الأساسية. فيجب النظر إلى الهيئات التنظيمية على أنها شريك أساسي ، لا لغرض الحفاظ على الامتثال فحسب، بل لضمان تنفيذ المتطلبات الأساسية بطريقة سلسة وتحديد جميع التحديات في المراحل الأوَّلية.

6. تحديد معدل المخاطر لجميع الأصول الرئيسية ووضع نهج حماية لكل أصل مع التركيز على الأصول الأكثر أهمية. يُعد تحديد مدى أهمية كل أصل مطلباً حاسماً لكل جهة حكومية؛ لأنه يترتب على ذلك تحديد مستوى الحماية للأصول. فحماية كل أصل داخل الجهة بالدرجة نفسها ليس نهجاً مجدياً، ولذا فإنه، من الضروري اتباع نهج أكثر واقعية ينظر إلى الخطر على أنه عنصر أساسي.

7. وضع نموذج ديناميكي وسريع الاستجابة لإدارة مخاطر الأمن الإلكتروني لتمكين الجهة الحكومية من توسيع نطاقه إذا كان هناك تصعيد للمخاطر الخارجية أو قرار لتغيير القدرة على تحمل المخاطر المؤسسية.

8. دمج الامتثال في استراتيجية الأمن الإلكتروني، بحيث تُعاد قيمة أي أموال مستثمرة في الامتثال من خلال توفير دفاع مناسب للجهة الحكومية.

9. تعزيز المرونة بوضع خطة عمل واتصال واضحة للأزمات بحيث يمكن التفكير ملياً في إدارة الأزمات والاستمرارية وممارستها على جميع مستويات الجهة الحكومية.

10. التعاون مع الأقران لإيجاد مزيد من الحلول داخل القطاعات. فالمخاطر الإلكترونية الحالية تهدد النظام البيئي الحكومي بأكمله، وقد يؤدي فشل أي من الجهات الفاعلة الرئيسية إلى الإضرار بسمعة المجال بأكمله.

وفي الختام، لم يعد كافياً النظر إلى المرونة في الأمن الإلكتروني على أنها فكرة مستدركة. يجب تضمين نهج الجيل التالي للحوكمة والمخاطر والامتثال في نظام الحصانة الخاص بالحكومة والجهات الحكومية بوصفه درع حماية في عالم يسوده انعدام اليقين وتتزايد فيه التهديدات الإلكترونية.

المراجع

1. https://www.ey.com/en_vn/ey-global-information-security-survey-2021
2. Tom, Burt, 4 November 2022. "Nation-state cyberattacks become more brazen as authoritarian leaders ramp up aggression," Microsoft Corporate Vice President, Customer Security & Trust (Burt, 2022).
3. Link to reference: https://www.crowdstrike.com/resources/reports/global-threat-report/
   Direct link to report: https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2022GTR.pdf
4. https://thehackernews.com/2022/12/chinese-hackers-target-middle-east.html
5. https://www.securitymagazine.com/articles/97549-winnti-apt-group-stole-trillions-in-intellectual-property
6. https://blogs.microsoft.com/on-the-issues/2022/11/04/microsoft-digital-defense-report-2022-ukraine/
7. https://www.nist.gov/news-events/news/2022/05/nist-updates-cybersecurity-guidance-supply-chain-risk-management
8. https://www.federalregister.gov/documents/2019/11/27/2019-25554/securing-the-information-and-communications-technology-and-services-supply-chain
9. https://www.interpol.int/News-and-Events/News/2021/Immediate-action-required-to-avoid-Ransomware-pandemic-INTERPOL
10. https://blogs.microsoft.com/on-the-issues/2022/11/04/microsoft-digital-defense-report-2022-ukraine/
11. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf, 21 September 2021
12. https://www.fincen.gov/news/news-releases/fincen-provides-financial-institutions-red-flags-potential-russian-sanctions, 07 March 2022
13. https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-annual-munich-cyber-security
14. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_5634
15. https://www.congress.gov/bill/117th-congress/senate-bill/965
16. https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/code-of-practice
17. https://www.cisa.gov/circia
18. https://www.sec.gov/news/press-release/2022-39
19. https://www.congress.gov/bill/117th-congress/senate-bill/2629/text

المساهمون

سامر محمد عمر
مدير أول، استشارات التكنولوجيا
Ernst & Young for Systems and Programming WLL (Branch)
samer.m.omar1@sa.ey.com

سلام شومان
قائد فريق، استشارات التكنولوجيا
Ernst & Young Jordan
salam.shouman@jo.ey.com

فادي موسى
قائد، استشارات التكنولوجيا
Ernst & Young for Systems and Programming WLL (Branch)
fadi.mousa1@sa.ey.com

سيدهش مدباتكال
مدير، استشارات التكنولوجيا
Ernst & Young Ltd, Mauritius
siddhesh.mudbhatkal@mu.ey.com

إياد حداد
مدير، استشارات التكنولوجيا
Ernst & Young for Systems and Programming WLL (Branch)
eyad.haddad1@sa.ey.com

إدمارك م بيلونز
مدير، استشارات التكنولوجيا
EY consulting LLC (Abu dhabi branch)
edmark.m.billones@ae.ey.com

شذى المطيري
مدير، استشارات التكنولوجيا
Ernst & Young for Systems and Programming WLL (Branch)
shatha.almutairi@sa.ey.com

مصعب أبو طه
مستشار أول، استشارات التكنولوجيا
Ernst & Young Jordan
musab.abutaha@jo.ey.com

ياسمين عبد الله
مستشار أول، استشارات التكنولوجيا
Ernst & Young Jordan
yasmeen.abdullah@jo.ey.com

شوكت النابلسي
مستشار أول، استشارات التكنولوجيا
Ernst & Young Jordan
shawkat.alnabulsi@jo.ey.com

إرنست ويونغ | بناء عالم أفضل للعمل

تعمل إرنست ويونغ من أجل بناء عالم أفضل للعمل من خلال المساعدة في خلق قيمة طويلة الأجل للعملاء والموظفين والمجتمع وبناء الثقة في الأسواق المالية.

توفر فرق إرنست ويونغ المتنوعة التي تعمل في أكثر من 150 بلداً، وبما تملكه من بيانات وتقنية، الثقة من خلال التدقيق المالي ومساعدة العملاء على النمو والتحول.

كما تقوم فرقنا، ومن خلال عملها في التدقيق المالي والخدمات الاستشارية ومجال القانون والاستشارات الاستراتيجية والاستشارات الضريبية والمعاملات التجارية بطرح الأسئلة الأفضل للتوصل إلى إجابات جديدة بشأن المشكلات المعقدة التي تواجه عالمنا اليوم.