إعادة موازنة المخاطر

خمسة أسئلة مهمة للمخاطر الجيوسياسية لرؤساء المعلومات[1]

ياسر فنري

ماجستير في العلوم المالية والمصرفية - مدير مالي

يحتاج الرؤساء التنفيذيون لشؤون المعلومات إلى تطبيق رؤية أوسع بكثير لأنماط الفشل المحتملة، وأين توجد أصولهم، وأين يعمل الأشخاص الذين يديرون الأصول.

خلال أيام ذروة "العالم مسطح" في التسعينيات وأوائل العقد الأول من القرن الحادي والعشرين، وعدت العولمة بكفاءة وفرص جديدة. خلال تلك الفترة، أعاد الرؤساء التنفيذيون لشؤون المعلومات بناء وظائفهم التكنولوجية للاستفادة من البنية التحتية الموزعة والشبكات العالمية ومراكز المواهب لتحسين الكفاءة وخفض التكاليف. قاد دافع العولمة هذا الشركات إلى تخصيص قدراتها في مجال تكنولوجيا المعلومات للأسواق المحلية، مما أدى إلى إنشاء مؤسسات تكنولوجيا معلومات مجزأة ومعقدة للغاية مع أشخاص وأصول منتشرة في جميع أنحاء العالم.

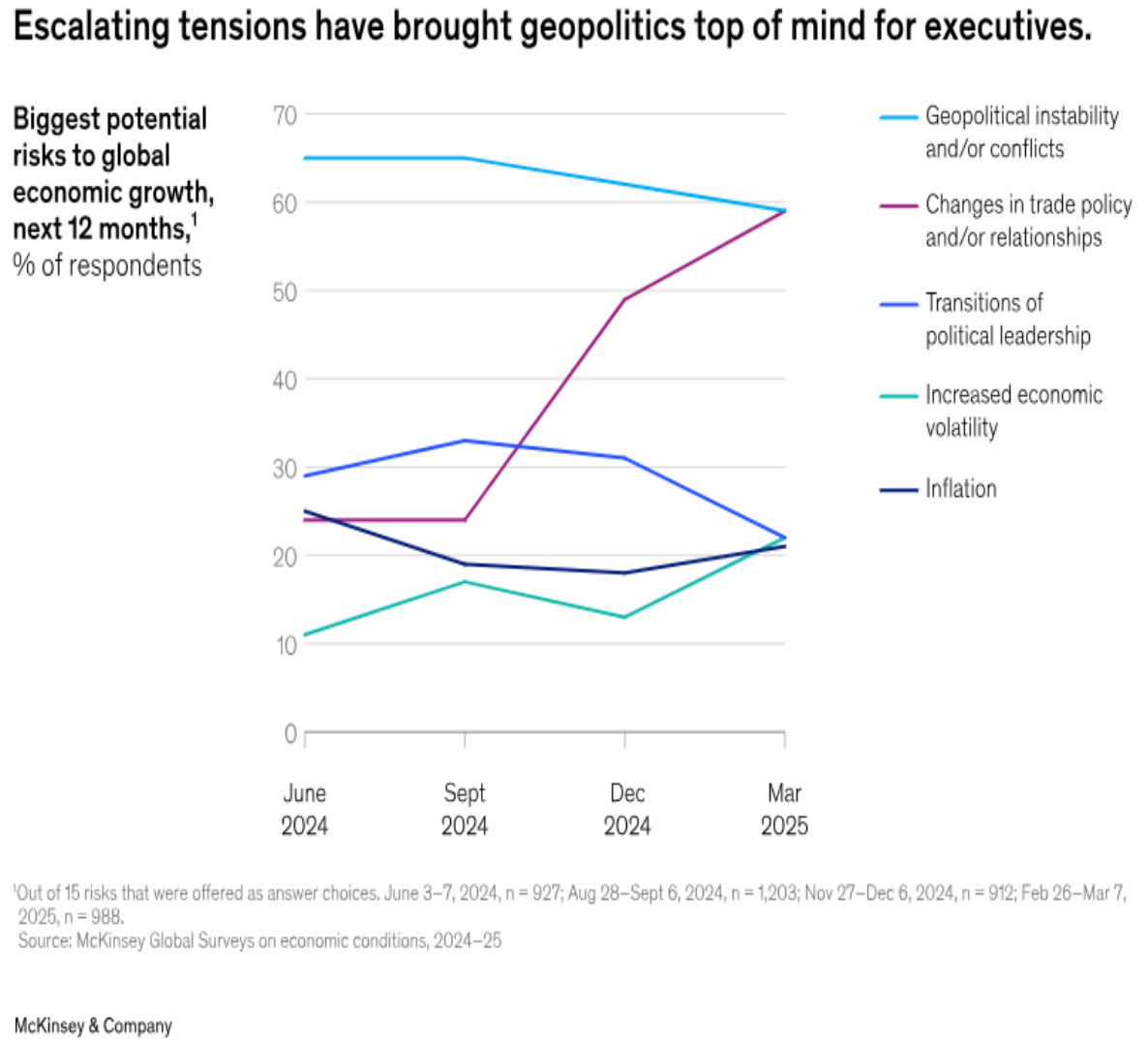
ومع ذلك، في العقد الماضي، وضعت التطورات الجيوسياسية نموذج تشغيل تكنولوجيا المعلومات العالمي هذا تحت ضغط هائل. أكثر من ٧٠٪ من البلدان لديها قوانين حماية البيانات وقوانين الخصوصية الخاصة بها، ومدى تأثير القوانين الجيوسياسية على خصوصية البيانات والتوافق التنظيمي في دول قد تغير سياساتها فجأة (مثلاً، قوانين الرقابة أو الوصول الحكومي) والتعارض بين تشريعات الدول في قوانين مراقبة البيانات كالصين أو روسيا. فتصاعدت سرقة البيانات والهجمات الإلكترونية، بعضها بتوجيه من الدول. في الواقع، تبلغ الأضرار السنوية المتوقعة من الهجمات الإلكترونية حوالي ١٠.٥ تريليون دولار خلال عام ٢٠٢٥ – بزيادة قدرها ٣٠٠٪ عن مستويات عام ٢٠١٥. كما أدت السياسات الصناعية والتجارية التي تفضل مقدمي الخدمات المحليين إلى زيادة الاعتماد على العمليات المحلية، مما زاد من تعقيد وتكلفة مشتريات تكنولوجيا المعلومات وعملياتها.

[1] نشر بواسطة ماكينزي ديجيتال بتاريخ 05 مايو 2025، ترجمة بتصرف في مقال بحثي للسادة (جايمس كابلان، جان شيلي براون، وتكير بايلي)، رابط.

في الوقت الحالي لا ترقى سياسات ونماذج تكنولوجيا المعلومات بشكل عام إلى مستوى مهمة معالجة نطاق (ووتيرة) المخاطر الجيوسياسية. نظرًا لتزايد الارتباط بين التكنولوجيا والسياسة الدولية فسيحتاج الرؤساء التنفيذيون لشؤون المعلومات الذين يأملون في التغلب بنجاح على هذه التحديات إلى مراجعة ممارسات المخاطر الحالية الخاصة بهم، وتطوير ممارسات جديدة، وإعادة التوازن إلى بصمتهم العالمية ونموذج تشغيلهم. يتضمن ذلك التواجد على الطاولة مع قيادة الأعمال للمساعدة في تشكيل القرارات حول المخاطر الجيوسياسية ليس فقط من حيث الآثار المترتبة على ملكية التكنولوجيا، ولكن أيضا من حيث الآثار المترتبة على المخاطر التقنية على الشركة نفسها.

أصبحت المخاطر الجيوسياسية قضية رئيسية للمديرين التنفيذيين، مما يخلق زخما ودعما واسعين لقادة التكنولوجيا لمعالجة هذه القضايا فقد جعلت التوترات المتصاعدة الجغرافيا السياسية على رأس أولويات المديرين التنفيذيين (الشكل ١).

يوفر الإجراء المدروس للشركات ميزة المحرك الأول من خلال تأمين البيانات أو الموقع أو خيارات المواهب عندما يكون التسعير على الأرجح أفضل مما سيكون عليه في وقت حدوث الخطر عندما تتدافع الشركات للتنافس على الموارد النادرة. في كثير من الحالات، تفكر الشركات بالفعل في كيفية إعادة التوازن إلى قواعدها التكنولوجية من خلال دمج المخاطر الجيوسياسية في قرارات الرؤساء التنفيذيين لشؤون المعلومات لاتخاذ إجراءات أكثر فعالية.



الشكل (١)

١ – أين توجد الأصول والأشخاص الأكثر أهمية للأعمال، ومدى تعرضهم للقوى الجيوسياسية؟

النظرة الوظيفية التقليدية لأهداف المخاطر التقنية – مثل التوافر والتسليم ووقت التشغيل – ليست كافية لمعالجة المخاطر الجيوسياسية. قد تجتاز الشركة اختبار هجوم إلكتروني، ولكن ليس اختبار تركيز الأصول، على سبيل المثال. يحتاج الرؤساء التنفيذيون لشؤون المعلومات إلى تعزيز وجهات نظرهم حول المخاطر من خلال تطوير رؤية أوسع بكثير لأنماط الفشل المحتملة بما يتجاوز مجرد التوافر والاستمرارية (على سبيل المثال، سرقة البيانات، وإدخال التعليمات البرمجية أو البيانات الضارة، والتلاعب)، وأين توجد أصولهم (وأصول بائعيهم)، وأين يعمل الأشخاص الذين يديرونها.

لكي يكون المديرون التنفيذيون لشؤون المعلومات ومديرو التكنولوجيا هادفين وعمليين، يحتاجون إلى التركيز على الأصول والفرق التي تدعم وظائف الأعمال الهامة ولديهم رؤية دقيقة بما فيه الكفاية لأصولهم وموظفيهم لفهم نقاط الضعف الحقيقية لشركاتهم. من خلال الدول التي يعتمد على بنيتها التحتية الرقمية أو مزودي الخدمات السحابية مثل AWS، Azure، Alibaba Cloud إذا الشركة تنشط في مناطق ذات توترات سياسية وعليها عقوبات أو قيود مفروضة، وكمية المخاطر المرتبطة بسلاسل التوريد وتوافر خطة بديلة في حال تعطل الإمدادات إذا كان الموردون يستخدمون تقنيات أو مكونات مصدرها دول ذات مخاطر جيوسياسية بسبب النزاعات أو العقوبات، كما يحتاج الرؤساء التنفيذيون لشؤون المعلومات إلى فرز ممتلكاتهم التقنية لتطوير رؤية ٨٠ / ٢٠ لما يهم الأعمال. إذا تعطل نظام يدير قوائم طلبيات كافيتريا الشركة، أو تعطل النظام الذي يتتبع الأيام المرضية للموظفين، فيمكن للشركة إدارتها. ولكن إذا تعطل النظام الذي يدير المدفوعات أو مبيعات التجارة الإلكترونية، فسيكون ذلك كارثيا على الأعمال. هذه هي الأنظمة والقدرات التي يحتاج الرؤساء التنفيذيون لشؤون المعلومات إلى التركيز عليها. كتأثير سياسات الهجرة والتأشيرات على قدرة الشركات على توظيف المهارات التقنية.

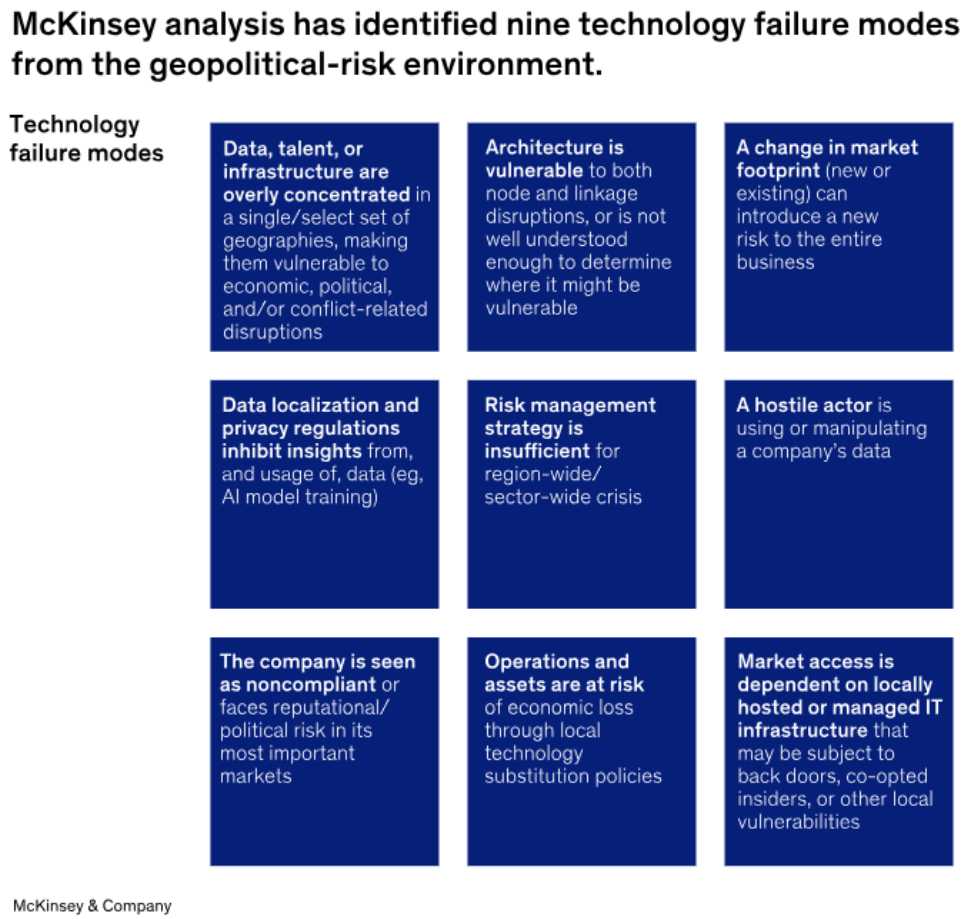
ومع ذلك، فإن فهم الطبيعة الحقيقية لنقاط الضعف في تلك الأنظمة ذات الأولوية العالية يتطلب من الشركات أن يكون لديها فهم مفصل بما فيه الكفاية لتدفقات القيمة (مجموعة العمليات الشاملة اللازمة لتحقيق نتيجة) . هذا صحيح بشكل خاص في عالم تكون فيه المقرات التقنية معقدة للغاية وتعتمد على البائعين (وبائعي بائعيهم) في أجزاء منها.

بالنسبة لدورة حياة تطوير منتج مصرفي استهلاكي جديد، على سبيل المثال، تعد التكنولوجيا أحد مكونات كل مرحلة: التصميم والاختبار، والإنتاج، والتوسع، والتوزيع. سيحتاج البنك الاستهلاكي إلى تحديد كل أصل تقني، أو عقدة، على طول دورة الحياة هذه وفهم مكانها وما هي المتطلبات المحلية. في هذه الحالة، قد يعني ذلك معرفة أن قاعدة البيانات اللازمة لاختبار منتج ما موجودة في الصين وتخضع للوائح البلاد.

٢ – ما الذي يمكن أن يحدث – أو يحدث بالفعل – بشكل خاطئ؟

إن الزيادة في العناوين الرئيسية حول الصراع العالمي وعدم الاستقرار التجاري وتصاعد اللوائح المتعلقة الذكاء الاصطناعي والبيانات تعني أن العديد من مدراء تقنية المعلومات ومديري التكنولوجيا يفكرون بالفعل في أوضاع فشل مختلفة. ومع ذلك، فإن القضية الرئيسية هي أن هذه الاعتبارات تميل إلى أن تكون تفاعلية ومحدودة النطاق، مما يخلق نقاطا عمياء للتخفيف من المخاطر الجيوسياسية. على وجه التحديد، يجب على قادة التكنولوجيا تقييم تسعة أنواع من أنماط الفشل التي تنبع من المخاطر الجيوسياسية، بما في ذلك البنية المعرضة لتعطيل العقدة والارتباط، والأصول المركزة بشكل مفرط في منطقة جغرافية واحدة أو بضع مناطق جغرافية معينة، والبصيرة الثاقبة من البيانات واستخدامها بسبب لوائح الخصوصية (الشكل ٢).

حدد تحليل ماكينزي تسعة أوضاع للفشل التكنولوجي الناجم عن بيئة المخاطر الجيوسياسية.



الشكل (٢)

تصبح أوضاع الفشل هذه خط الأساس لتطوير سيناريوهات التطوير المنهجي لتدفقات القيمة ذات الأولوية. تأخذ هذه السيناريوهات في الحسبان البصمة الجغرافية ويتم إبلاغها بمخاوف تشغيلية محددة أو التوترات الجيوسياسية المتصاعدة (مثل الحواجز التجارية الناشئة) التي قد يرغب رئيس قسم المعلومات في إجراء مزيد من التحقيق. في بعض الحالات، تقوم الشركات بتكليف سيناريوهات مصممة بدرجة عالية من متخصصين في المخاطر الجيوسياسية للمساعدة في تجسيد الخيارات.

من المهم أن ندرك أن بعض أوضاع الفشل هذه ليست مرتبطة ببساطة بالسيناريوهات المحتملة المستقبلية، ولكنها تحدث بالفعل وتحتاج إلى معالجة. بعض الشركات معرضة بالفعل لخطر سرقة البيانات أو عنوان ال IP، على سبيل المثال، بحكم مكان عملياتها. أو تهديدات سيبرانية ترعاها دول قد تستهدف الشركة أو عملياتها أو إذا تم تقييد الوصول إلى الإنترنت أو الشبكات العالمية

٣ – ما هي الخطة التي يجب اتباعها عند وقوع حدث جيوسياسي؟

عادة، لا تقوم الشركات بوضع نماذج تأثير مخاطر جيوسياسية معينة بشكل مسبق وعند حدوثها يكون الأوان قد فات للتخفيف من الضرر لأن الطبيعة البطيئة للتكنولوجيا تجعل من الصعب التدخل بسرعة. لهذا، يخطط مدراء تقنية المعلومات ذوو التفكير المستقبلي بشكل استباقي للتدخلات بناء على السيناريوهات التي طوروها.

تحدد أفضل خطط التدخل نطاق علامات التحذير المتصاعدة وتضع مجموعة من الإجراءات المقابلة التي يمكن للشركات اتخاذها للرد بعناية مع الحفاظ على أكبر مجموعة ممكنة من الخيارات. عندما يتم ذلك بشكل جيد، ينتج عن تخطيط التدخل هذا مجموعة متتالية من المحفزات والإجراءات التي تتبع مسار تصعيد محدد (الشكل ٣).

من خلال تحديد التدخلات، يمكن لمدراء تقنية المعلومات التحرك بسرعة أكبر من المنافسين عند حدوث خطر وتأمين اتفاقيات أكثر فعالية من حيث التكلفة مما ستكون عليه عند التدافع في مواجهة حدث خطر. يمكنهم أيضا الاستثمار في التطوير التكنولوجي الضروري بطريقة مدروسة وفعالة من حيث التكلفة بدلا من الرد البحت على الأحداث لمرة واحدة.

ربط تدابير التخفيف الاستباقية والتفاعلية بمراحل التصعيد الجيوسياسي للخطر.

الشكل (٣)

٤ – ما هي خطوات التخفيف التي يجب على الرؤساء التنفيذيين لشؤون المعلومات اتخاذها؟

للحفاظ على وضع المخاطر الفعال، تحتاج الشركات إلى إعادة توازن عملياتها على مستوى العالم لمعالجة المشكلات الحالية والمحتملة. لدى الرؤساء التنفيذيين لشؤون المعلومات الكثير من خيارات التخفيف من المخاطر، مثل تخصيص أموال الطوارئ للطوارئ قصيرة الأجل، وإعادة توجيه العمليات إلى المناطق الأقل خطورة، وتكرار العمليات لخلق التكرار، وتوطين العمليات العالمية في وحدات خاصة بالمنطقة. ومع ذلك، فإن شكل إعادة التوازن هذا سيعتمد على التفكير في الخيارات التي تعالج المخاطر بشكل أفضل وما إذا كانت تستحق الاستثمار والخسارة في الإنتاجية.

اتباع نهجًا عالميًا:

قد يكون من المغري إنشاء استراتيجية على مستوى البلد أو المنطقة لضمان الامتثال للوائح المحلية (على سبيل المثال، اللائحة العامة لحماية البيانات، ومعايير Schrems II القائمة على القرار، وقانون حماية المعلومات الشخصية الصيني) . ومع ذلك، قد يكون لهذا النهج تأثير دفع المخاطر عن غير قصد إلى مناطق جغرافية أخرى (يعرف أيضا باسم "الضغط على البالون") .

قد تختار شركة متعددة الجنسيات تجنب المخاطر في بلد ما عن طريق نقل مركز بيانات موجود إلى منطقة أخرى لديها مجموعة من المخاطر الجيوسياسية الخاصة بها، كإنشاء استراتيجية متعددة السحب (Multi Cloud Strategy) لتقليل المخاطر الإقليمية وقد تخلق إجراءات التخفيف تعقيدات وتكاليف كبيرة تفوق فوائدها . على سبيل المثال، انتهى الأمر بإحدى الشركات الاستهلاكية إلى بناء أكثر من ٨٠ مركزا للبيانات للحد من قضايا المخاطر الجيوسياسية المحلية، وهو مشهد مجزأ للغاية خلق تعقيدا تشغيليا هائلا وكان ببساطة لا يمكن الدفاع عنه .

الفحص المسبق للموردين الاستراتيجيين وسلاسل التوريد ضد قوائم الحظر الدولية .

إعادة التوازن الأرضي على أساس تحليل واضح للتكلفة والعائد :

بنفس الطريقة التي يأخذ بها المديرون الماليون في الاعتبار المخاطر من خلال دمج تكلفتها في التخطيط المالي، يحتاج الرؤساء التنفيذيون لشؤون المعلومات إلى تكلفة المخاطر المحتملة واستراتيجيات التخفيف للسماح بتحليل مدروس للتكلفة والفائدة . باستخدام النمذجة المالية وتحليل البيانات، يمكن لرئيس قسم المعلومات العمل مع المدير المالي، وكبير مسؤولي أمن المعلومات، وكبير مسؤولي الموارد البشرية، وقادة البنية التحتية لتطوير رؤية متسقة لاستراتيجيات التخفيف الأكثر منطقية بالنظر إلى التكاليف والفوائد . من المحتمل أن تتطلب هذه الممارسات من الشركات إعادة بعض مكاسب كفاءة تكنولوجيا المعلومات من العولمة مقابل ليس فقط المزيد من المرونة، ولكن أيضا لمزيد من المرونة الاستراتيجية .

في حين أنه من غير الواقعي توقع أن يؤدي هذا التحليل إلى حسابات مثالية، إلا أن القيمة تكمن في وجود رؤية واضحة ومتوافقة للإجراءات الأكثر منطقية لمجموعة من المخاطر . من خلال التجربة، يمكن للشركات أن تتوقع تحسين هذه التحليلات وتحسينها .

بناء المرونة في ملكية تكنولوجيا المعلومات :

قد تكون ترقية ملكية تكنولوجيا المعلومات مكلفة، لذلك يجب أن يكون الرؤساء التنفيذيون لشؤون المعلومات حذرين مع الإجراءات التي يتخذونها كجزء من برنامج إعادة التوازن الأوسع وعدم المبالغة في رد الفعل. يجب على مدراء تقنية المعلومات استثمار الوقت لتحديد المكونات التي يمكن تخصيصها أو توحيدها بناء على احتياجات المخاطر والتكنولوجيا المتاحة (مثل واجهات برمجة التطبيقات والخدمات المصغرة). وتطوير اتفاقيات حماية البيانات (DPA) مع كل مزود خارجي، كما ينبغي أن ينصب التركيز على توحيد نظم البنية التحتية الأساسية ونماذج النشر مع توفير التباين في كيفية إنشاء المنصات ومنتجات البيانات استنادا إلى اللوائح الإقليمية والحد من التهديدات السيبرانية الهجومية سواء أكانت شخصية أم مدعومة من قبل جهات قد ترقى لتكون حكومية مثل (SolarWinds) الروسية أو (Hafnium) الصينية.

العنصر الأساسي لهذه الإمكانية هو بنية النظام الأساسي المكونة من مكونات يمكن للفرق المحلية تكوينها أو الاتصال بها من خلال واجهات قياسية مطورة مركزيا (مثل واجهات برمجة التطبيقات). يعتمد نجاح هذا النموذج على المواءمة حول التوازن الصحيح بين القدرات العالمية والمحلية وهياكل الحوكمة الواضحة لتوضيح حقوق القرار والاستثمار في تقنيات EDR / XDR ومنصات SIEM القادرة على اكتشاف الهجمات المستهدفة المعقدة.

على سبيل المثال، وجدت شركة استهلاكية متعددة الجنسيات أن المشهد التنظيمي سريع التغير في الصين جعل من الصعب عليها بشكل متزايد تقديم تجربة عملاء محلية من الدرجة الأولى بكفاءة بسبب بنيتها التقنية العالمية. من خلال إنشاء فريق دعم ومجموعة تقنية محلية تلتزم باللوائح المحلية، ولكنها تستخدم قدرات مثل واجهات برمجة التطبيقات للاستفادة من المنصة العالمية، يمكن للشركة تلبية احتياجات المستهلكين الصينيين بشكل أفضل مع الحفاظ على الامتثال.

على الرغم من أن تصميم هندسة معمارية محلية متوافقة كان من بعض النواحي هو الجزء السهل للشركة. جاء العمل الحقيقي من الفصل المدروس بين بيانات أعمالها والمستخدمين لضمان بيئة خصوصية بيانات عالمية أكثر أمانا، مع قواعد واضحة لتجميع البيانات والإقامة عبر بصمتها العالمية.

٥ – هل الأشخاص المناسبون وعمليات الحوكمة موجودة لاتخاذ الإجراءات؟

قد يبدو من غير المناسب القول إن النماذج التقليدية لارتباط مخاطر تكنولوجيا المعلومات لم تعد كافية لحساب المخاطر الجيوسياسية. ومع ذلك، فإن الآثار المترتبة أكثر تعقيدا من مجرد إضافة هذا الخطر كبند إلى برامج المخاطر الحالية. يبدأ تطوير هذه القدرة ببناء نظام جديد لمخاطر تكنولوجيا المعلومات، مع وضوح حول الأدوار والمسؤوليات وأي أحداث مخاطر جيوسياسية محتملة (الشكل ٤).

القادة الرئيسيون والرؤساء الوظيفيون لديهم مجالات مسؤولية مميزة عندما يتعلق الأمر بإدارة المخاطر الجيوسياسية.

Key leaders and functional heads have distinct areas of responsibility when it comes to managing geopolitical risk.

Roles and responsibilities for geopolitical-risk capability

Components of tech stack	Key owners	Potential geopolitical risk
Management/ governance	CIO, CTO	Armed conflict prompts strategic withdrawal from market Trade policies that could impact tech procurement or partnerships
Labor and support	Human resources	Changes in labor laws or employment standards in different countries Disruptions affecting ability to hire or relocate talent across borders
Cybersecurity	Chief information security officer	State-sponsored cyberattacks that may target critical infrastructure/data Escalating geopolitical tensions that can prompt cyberthreats
Network	Network administrators/engineers	Vulnerabilities in network equipment from specific countries Geopolitical conflicts that can interrupt international data transmission or network reliability
Cloud infrastructure/ platforms	Cloud architects/ engineers	Changes in data sovereignty laws (where data can be stored and processed) Sanctions and trade restrictions that can affect cloud service providers
On-premises infrastructure/ platforms	System administrators	Supply chain disruptions Import/export controls on technology components
Software	Software development managers, product managers	Changes in intellectual property laws or enforcement in different countries Regulatory compliance affecting software usage or data protection
Data and analytics	Data scientists and analysts	Data localization laws Cross-border data flows (eg, due to geopolitical tensions)
End user devices	IT support managers or desktop support specialists	Trade wars affecting availability and cost of end user devices Geopolitical instability that can affect distribution of hardware to end users

McKinsey & Company

الشكل (٤)

المخاطر الجيوسياسية مترابطة بطبيعتها، حيث من المحتمل أن تكون أجزاء متعددة من الأعمال ناتجة عن حدث جيوسياسي واحد، لذلك يجب دمج القدرة عبر الوظائف والممارسات. يكمن أحد عناصر هذا التكامل في تكنولوجيا المعلومات نفسها، حيث تمت إدارة وظائف مخاطر تكنولوجيا المعلومات التقليدية (مثل التوافر والمرونة، والأمن السيبراني، وحماية البيانات والملكية الفكرية، والتعرض

التنظيمي، وتركيز المواهب التقنية) بشكل مستقل. تتفاقم مشكلة المخاطر الجغرافية إذا لم تفهم الشركات مواقع تجمعات البائعين (وتركيزات مواقع البائعين الذين يستخدمهم هؤلاء البائعون، والتي تسمى أحيانا "مخاطر الطرف التاسع") .

وينبغي أن تشرف القدرة الموحدة لإدارة الأصول والخدمات على هذه المهام. وتكون هذه القدرة مسؤولة عن قياس المخاطر والإبلاغ عنها عبر كل مكون على حدة، وتجميع ملف تعريف المخاطر هذا، وترجمة المشكلات العالقة إلى مصطلحات تجارية.

يجب أن يحدث هذا التكامل على مستوى المنظمة أيضا. إلى الحد الذي يكون فيه لدى الشركات برنامج مخاطر جيوسياسية، فإن تجربتنا هي أنه يميل إلى التركيز على قضايا سلسلة التوريد بدلا من قضايا تكنولوجيا المعلومات. لا يرتبط الرؤساء التنفيذيون لشؤون المعلومات ارتباطا كاملا بممارسات المخاطر الجيوسياسية للمؤسسات الأوسع. والنتيجة هي أن الرؤساء التنفيذيين لشؤون المعلومات يفتقرون إلى إطار عمل لتحديد المخاطر الجيوسياسية وإدارتها وتتبعها كجزء من برنامج أوسع على مستوى الشركة.

لكي تكون قائدا فعالا في برنامج المخاطر على مستوى المؤسسة، يجب على الرؤساء التنفيذيين لشؤون المعلومات التفكير في بناء فريق صغير ومتفاني لتتبع التطورات الجيوسياسية، وتقييم آثارها وتأثيرها، وتقديم توصيات للقادة مع الوقت الكافي لاتخاذ الإجراءات. هذا هو المكان الذي تكون فيه القدرة الموحدة لإدارة الأصول والخدمات أمرا بالغ الأهمية. والتخطيط لاستمرارية الأعمال (BCP) في حال النزاعات وتحديثها واختبار القدرة على العمل بدون الوصول إلى مواقع أو خدمات سحابية معينة

يجب على الشركة دمج هذا الفريق في وظائف إدارة المخاطر الحالية، بما في ذلك السجلات وخطط العلاج، مع إطار عمل وبروتوكولات واضحة لفهم كيف وأين تساهم البيانات والعمليات التقنية في عقد متميزة في سلسلة قيمة الأعمال. يمكن أن تتغير البيئة الجيوسياسية بسرعة، لذلك ستحتاج المؤسسات إلى تحديث تحليلاتها واستجاباتها للمخاطر. يحتاج الرؤساء التنفيذيون لشؤون المعلومات ومديرو التكنولوجيا إلى تقييم المخاطر الجيوسياسية باستمرار.

تظل القوى الجيوسياسية التي تشكل الأعمال والاقتصاد مائعة وديناميكية. قلة هم الذين يمكنهم التنبؤ بثقة بالاتجاه الذي قد يتحول إليه المد والجزر، ولكن هناك فرصة جيدة لأن يكون عدم اليقين والمخاطر الجيوسياسية المتزايدة هي القاعدة في المستقبل القريب. لا يمكن لقادة التكنولوجيا الذين يمكنهم التغلب

على هذا التقلب حماية أعمالهم فحسب، بل يمكنهم أيضا التفوق على منافسيهم ولعله من المهم أن نوصي بالتعاون مع خبراء في الأمن الجيوسياسي أو الاستعانة بتقارير خارجية منتظمة عن الأحداث الجيوسياسية وتأثيرها المحتمل على التكنولوجيا .