مخاطر الأمن السيبراني: مخاوف متزايدة إزاء الاستقرار المالي الكلي

على خلفية نمو التحول الرقمي وتطور التكنولوجيا وتزايد التوترات الجغرافية–السياسية، أصبحت حوادث الأمن السيبراني، ولا سيما المرتكبة بدافع الضرر، أكثر تواترا خلال العقدين الماضيين، وتحديدا منذ عام ٢٠٢٠. ويمكن أن تنشأ عن الحوادث الجسيمة في كبرى المؤسسات المالية تهديدات حادة للاستقرار المالي الكلي من خلال فقدان الثقة، وتعطل الخدمات الحيوية، وانتشار التداعيات إلى المؤسسات الأخرى عبر الروابط التكنولوجية والمالية.

ويوضح الفصل أنه بالرغم من أن حوادث الأمن السيبراني لم تؤثر على النظام ككل حتى الآن، أصبحت الشركات أكثر عرضة لخطر الخسائر الفادحة المباشرة – التي تصل إلى ٢,٥ مليار دولار أمريكي على الأقل – الناجمة عن تلك الحوادث. وعلاوة على ذلك، تنشأ عن حوادث الأمن السيبراني خسائر غير مباشرة هائلة أيضا، والتي عادة ما تتجاوز بكثير الخسائر المباشرة التي تعلنها الشركات.

واستيعاب العوامل المساهمة في وقوع حوادث الأمن السيبراني أو الوقاية منها هو عنصر ضروري لوضع سياسات واستراتيجيات قوية لحماية الأمن السيبراني. وحسب التحليلات الواردة في الفصل، نتجت عن التحول الرقمي والتوترات الجغرافية–السياسية زيادة هائلة في خطر الحوادث السيبرانية، بينما قد تساعد التشريعات السيبرانية الأكثر تطورا وتحسين الحوكمة السيبرانية في الشركات على التخفيف من هذه المخاطر.

والقطاع المالي عرضة للمخاطر السيبرانية إلى حد كبير، حيث يبلغ نصيب الشركات المالية الخمس تقريبا من مجموع هذه الحوادث. وفي ظل ارتفاع التركز السوقي وتدني قابلية الإحلال، ولا سيما في القطاعات الخدمية الحيوية، مثل المدفوعات وخدمات صيرفة الحفظ الأمين، يمكن أن تتسبب الحوادث السيبرانية عبر الشركات المالية في اضطرابات هائلة، مما يؤكد أهمية تعزيز الأمن السيبراني وصلابة العمليات. وغالبا ما تعتمد عمليات الشركات المالية على نفس مقدمي خدمات تكنولوجيا المعلومات الخارجيين، مما يزيد أيضا من خطر الصدمات والتداعيات المشتركة.

ويمكن أن يؤدي حادث سيبراني جسيم في إحدى المؤسسات المالية إلى تقويض الثقة في النظام المالي، وربما تنشأ عنه موجة بيع عارمة في الأسواق أو سحب جماعي للودائع المصرفية في الحالات القصوى. ورغم أننا لم نشهد حتى الآن سحبا جماعيا للودائع إثر هجمات سيبرانية، تشير التحليلات التجريبية إلى خروج تدفقات محدودة من الودائع بوتيرة ثابتة إلى حد ما من البنوك الأمريكية الأصغر حجما عقب الهجمات السيبرانية.

ويجب على أطر السياسات والحوكمة أن تواكب المخاطر السيبرانية الهائلة والمتنامية التي تواجه النظام المالي العالمي. ويشير مسح تم إجراؤه على البنوك المركزية والسلطات الرقابية في اقتصادات الأسواق الصاعدة والاقتصادات النامية إلى أن أطر سياسات الأمن السيبراني لا تزال غير كافية في الغالب.

ويتعين تعزيز الحصانة السيبرانية للقطاع المالي من خلال وضع استراتيجيات وطنية فعالة لحماية الأمن السيبراني، وتصميم أطر تنظيمية ورقابية ملائمة، وبناء قوة عاملة تتمتع بالقدرات اللازمة في مجال الأمن السيبراني، وصياغة ترتيبات محلية ودولية لتبادل المعلومات. ولضمان مراقبة المخاطر السيبرانية بفعالية أكبر، ينبغي تعزيز آليات الإبلاغ عن حوادث الأمن السيبراني. وعلى الأجهزة الرقابية أن تعهد إلى أعضاء مجالس الإدارة بمسؤولية إدارة الأمن السيبراني للشركات المالية، وتبني الثقافة الملائمة للتعامل مع المخاطر، وتشجيع مفهوم "النظافة السيبرانية"، والتدريب

في مجال الأمن السيبراني والتوعية بأهميته. وللحد من الاضطرابات المحتملة الناجمة عن حوادث الأمن السيبراني، ينبغي للشركات المالية وضع إجراءات للاستجابة والتعافي واختبارها. وعلى السلطات الوطنية أيضا تصميم بروتوكولات للاستجابة وأطر لإدارة الأزمات، مع ضمان فعاليتها.

ويضطلع صندوق النقد الدولي بدور فعال في مساعدة البلدان الأعضاء على تعزيز أطر الأمن السيبراني من خلال برامج تقييم القطاع المالي ومبادرات بناء القدرات. وللاطلاع على التقرير بالكامل، يرجى الرجوع إلى النسخة الإنجليزية عبر الرابط التالي: http://IMF.org/GFSR-April2024.