ECES
المركز المصري
للدراسات الاقتصادية
The Egyptian Center
for Economic Studies

عدسة اقتصادية

العدد 27
20 سبتمبر 2026

تزايد مخاطر الأمن السيبراني: الشرق الأوسط، ومصر

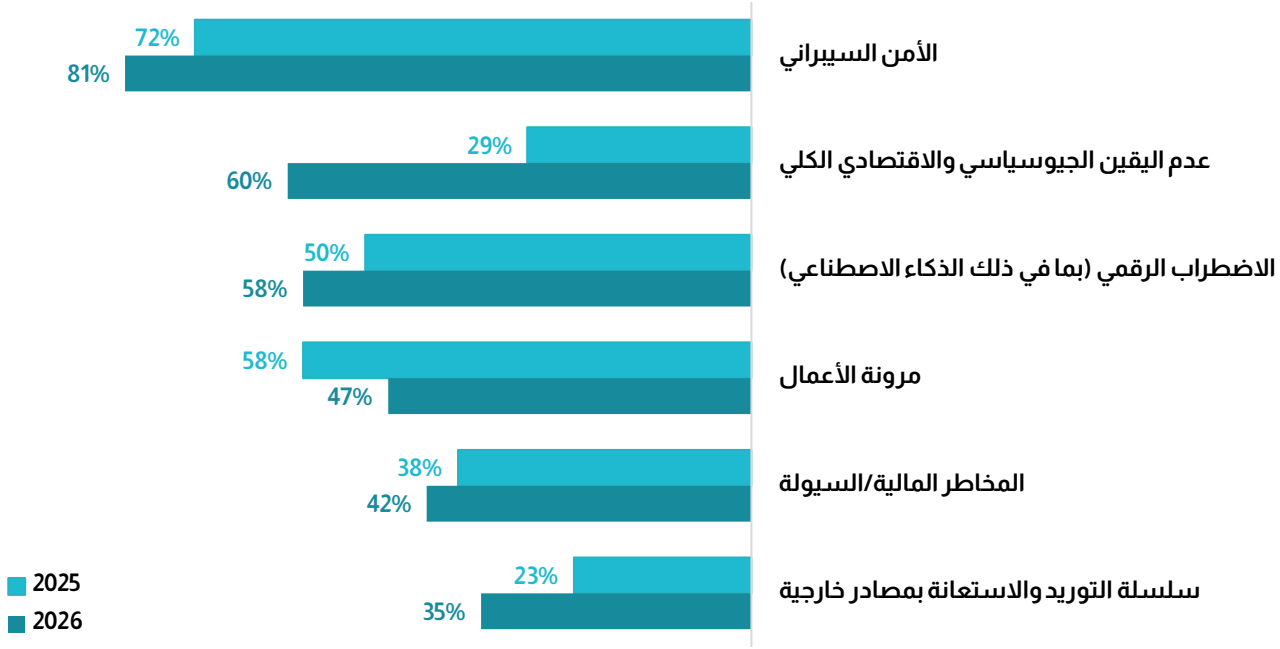
لماذا نتناول هذا الموضوع الآن؟

رغم هيمنة الحرب الإقليمية التي بدأت في فبراير 2026 على النقاش حول المخاطر في الشرق الأوسط، إلا أن مؤسسات المنطقة لا يصنفونها في المرتبة الأولى. فقد نشرت مؤسسة التدقيق الداخلي والاتحاد العربي للمراجعين الداخليين (ARABCIA) مؤخرا تقريرا بعنوان Risk in Focus 2026/2027: Middle East، وهو مسح سنوي يحدد أهم خمس مخاطر تواجه المؤسسات في كل منطقة من مناطق العالم.[1] ويستند إصدار عام 2026 إلى إجابات 3,285 شخص من كبار المسؤولين التنفيذيين في مجال التدقيق الداخلي في 132 دولة، من بينهم 296 مشاركا من 15 دولة في الشرق الأوسط. وبلغ عدد المشاركين في مصر 39 مشاركا، لتأتي بذلك في المرتبة الرابعة من حيث حجم العينة الوطنية في المنطقة، بعد عُمان والبحرين والإمارات. وبالإضافة إلى المسح، يستند التقرير كذلك إلى حلقتي نقاش إقليميتين بمشاركة 20 شخصا، بالإضافة إلى ثلاث مقابلات شخصية.

ويتناول التقرير 16 مجالا من مجالات المخاطر، وتتمثل أهم نتائجه في أن الصراع بين الولايات المتحدة وإسرائيل وإيران قد أعاد ترتيب المخاطر الإقليمية في المنطقة خلال عام واحد فقط؛ حيث تضاعفت تقريبا نسبة كبار المسؤولين التنفيذيين في مجال التدقيق الداخلي في الشرق الأوسط الذين وضعوا عدم اليقين الجيوسياسي والاقتصادي الكلي ضمن أهم خمس مخاطر لديهم، من 29% في عام 2025 إلى 60% في عام 2026، وهي أعلى نسبة مسجلة في أي منطقة في العالم. وتصدر الأمن السيبراني أبرز المخاطر في كلا العامين، وارتفعت نسبته بمقدار 9 نقاط مئوية لتصل إلى 81% في عام 2026.

[1] مؤسسة التدقيق الداخلي والاتحاد العربي للمراجعين الداخليين(ARABCIA) ، *Risk in Focus 2026/2027: Hot Topics for Internal Auditors, Middle East* (2026)

الشكل (1): الشرق الأوسط: أبرز المخاطر، 2025 مقارنةً بـ 2026
(نسبة الرؤساء التنفيذيين للتدقيق الداخلي الذين اختاروا كل خطر ضمن أعلى خمسة مخاطر)



المصدر: إعداد المركز المصري للدراسات الاقتصادية، استنادا إلى تقرير *أبرز المخاطر المؤسسية، 2026/2027*.

تأتي مخاطر الأمن السيبراني في المرتبة الأولى بين المخاطر في كل منطقة شملها المسح. وعلى المستوى العالمي، أدرج 80% من كبار المسؤولين التنفيذيين في مجال التدقيق الداخلي مخاطر الأمن السيبراني ضمن أهم خمسة مخاطر في عام 2026، بزيادة قدرها سبع نقاط مئوية مقارنة بعام 2025. وكما يتضح من الشكل (2)، تراوحت النسب بين 72% في منطقة آسيا والمحيط الهادئ و86% في أوروبا، مما يشير إلى أن النظرة إلى هذه المخاطر لا تعتمد على مستوى الدخل أو درجة النضج الرقمي في المنطقة؛ فوفقا للتقرير، فإن أكبر الزيادات السنوية في المخاطر سُجلت في أفريقيا (+11 نقطة مئوية)، وآسيا والمحيط الهادئ (10+ نقاط مئوية)، والشرق الأوسط (9+ نقاط مئوية). ويشير هذا التقارب إلى أن مخاطر الأمن السيبراني أصبح ينظر إليها الآن باعتبارها مخاطر هيكلية ملازمة للعمل في اقتصاد رقمي، وليس مجرد مصدر قلق خاص بقطاع أو منطقة بعينها.

ويبين التقرير إعادة ترتيب المخاطر؛ حيث تراجعت مخاطر مثل مرونة الأعمال والحوكمة والثقافة المؤسسية، ليس بسبب انخفاض أهميتها، وإنما لأن هناك مخاطر أكثر إلحاحا حلت محلها. وبالرغم من ذلك، لم يتراجع ترتيب مخاطر الأمن السيبراني وظلت الأعلى ترتيبا في المنطقة للعام الرابع على التوالي. ولا يقتصر الأمر على تصنيف الأمن السيبراني باعتباره أعلى المخاطر، بل إنه استمر في هذا الترتيب رغم ارتفاع المخاطر الجيوسياسية. في هذا الإطار، يلقي هذا العدد من "عدسة اقتصادية" الضوء على الأهمية الاقتصادية للأمن السيبراني، والوضع الحالي له في مصر والشرق الأوسط، وما يجب القيام به للحد من هذه المخاطر.

الشكل 2. الأمن السيبراني ضمن أعلى خمسة مخاطر حسب المنطقة، 2026
(نسبة الرؤساء التنفيذيين للتدقيق الداخلي)

المصدر: تقرير أبرز المخاطر المؤسسية، 2027/2026.

ما أهمية مخاطر الأمن السيبراني للاقتصاد؟

الأمن السيبراني هو حماية الشبكات والأنظمة والخدمات الرقمية من النفاذ غير المصرح به أو التعطيل أو التدمير؛ فعلى سبيل المثال، الهجمات ببرمجيات الفدية يمكنها تعطيل أنظمة الدفع لدى تجار التجزئة، مما يؤدي إلى توقف المبيعات تماما حتى لو لم تتم سرقة أي بيانات للعملاء، وهو ما يوضح أن حماية الأنظمة تكتسب أهمية مستقلة عن حماية المعلومات. وقد أصبحت هذه الحماية قضية اقتصادية، وذلك لاعتماد المدفوعات والتجارة والطاقة والخدمات اللوجستية والخدمات الحكومية الآن على البنية التحتية الرقمية. ومن ثم، حدوث هجوم سيبراني ناجح يمكن أن ينتج عنه تكاليف تتجاوز الشركة المتضررة، مثل تعطل الخدمات، وفقدان المعاملات، وتراجع الثقة في القنوات الرقمية؛ فوفقا لتقرير لشركة آي بي إم IBM حول تكلفة اختراق البيانات عام 2025، بلغ متوسط التكلفة العالمية لاختراق البيانات 4.44 مليون دولار، مقابل 3.86 مليون دولار في عام 2020.[2]

وعلى المستوى العالمي، سجلت هذه التكاليف مستويات هائلة؛ حيث تقدر شركة Cybersecurity Ventures التكلفة السنوية العالمية للجرائم السيبرانية بنحو 10.5 تريليون دولار في عام 2026، ومن المتوقع أن ترتفع إلى 15.63 تريليون دولار بحلول عام 2029.

وبينما يُنظر إلى الأمن السيبراني في أغلب الأحيان ما باعتباره تكلفة فنية، فإنه يمثل أيضًا شرطًا أساسيًا للتحول الرقمي والاستثمار. ويعتمد كل من الشمول المالي، والحكومة الإلكترونية، والتكنولوجيا المالية، وتبني الذكاء الاصطناعي على استعداد الأسر والشركات لاستخدام القنوات الرقمية. وكان اختراق الأنظمة من جانب أطراف خارجية ومن خلال سلاسل الإمداد السبب الأكثر شيوعًا للاختراقات في الشرق الأوسط، حيث شكّل 17% من الحوادث، مما يشير إلى أن أمن أي شركة يعتمد على أمن مورديها.[3] ومن ثم، يتسم الأمن السيبراني بخصائص البنية التحتية المشتركة، إذ يؤدي نقص الاستثمار من جانب بعض الشركات إلى تحميل شركات أخرى تكاليف إضافية.

[2] IBM, Cost of a Data Breach Report 2025

[3] IBM Newsroom MEA, "Cost of a Data Breach 2025: Middle East findings." Converted at the official peg of SAR 3.75 per U.S. dollar.

هل مخاطر الأمن السيبراني هي نفس مخاطر أمن البيانات؟

على الرغم من الخلط بين المصطلحين في أغلب الأحيان، إلا أنهما مختلفان من حيث المهام المنوطة بهما؛ فالأمن السيبراني يحمي الأنظمة والشبكات من الهجمات، بصرف النظر عما تحتويه من معلومات، بينما أمن وحماية البيانات معنيان بالمعلومات ذاتها، بما في ذلك الجهات المسموح لها بجمعها، ومكان تخزينها، ومدة الاحتفاظ بها، وما إذا كان يجوز نقلها إلى الخارج. ومن ثم، قد يكون لدى المؤسسة دفاعات قوية لحماية شبكاتها، ومع ذلك تسيء استخدام البيانات الشخصية أو تجمع منها أكثر مما يلزم، كما يمكن أن تلتزم بقواعد حماية البيانات بينما تظل عرضة لهجمات برمجيات الفدية ransomware .

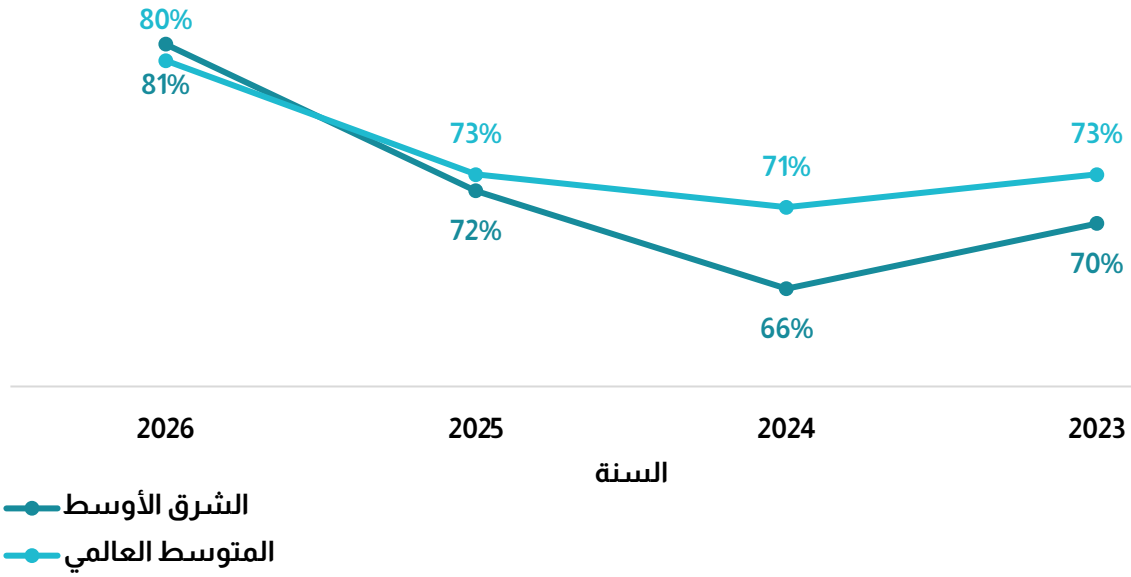
يتناول تقرير أبرز المخاطر المؤسسية هذا الفرق بين أمن البيانات والأمن السيبراني، وإن كان بصورة غير مباشرة. فالمسح يجمع بين المجالين، إذ يُعرف مجال المخاطر للمشاركين بأنه "الأمن السيبراني وأمن البيانات"، ما يعني أن نسبة 81% تشمل كليهما. ومع ذلك، يشير التقرير إلى أن الجهات التنظيمية في المملكة العربية السعودية طلبت من إحدى المؤسسات المالية الفصل بين منصبي المسؤول عن الأمن السيبراني والمسؤول عن أمن البيانات، وهو ما استلزم تعيين خبير إضافي من ذوي الخبرة في المناصب العليا. وأفاد المسؤول التنفيذي في مجال التدقيق الداخلي بأن تكاليف الامتثال المتعلقة بالأمن السيبراني ارتفعت بنسبة 40% خلال العام الماضي، ويرجع ذلك جزئيا إلى هذا المنصب الإضافي. كما يتناول التقرير حماية البيانات في إطار الاضطراب الرقمي، وليس ضمن الأمن السيبراني. ويشير إلى أن العديد من دول المنطقة تفرض قيودا على نقل البيانات عبر الحدود، وهو ما يتطلب في كثير من الأحيان الحصول على موافقة الجهات التنظيمية، فضلاً عن ضرورة الالتزام بمبدأ تقليل جمع البيانات إلى الحد الأدنى.

وترجع أهمية هذا الفصل بين المجالين إلى ثلاثة أسباب: أولا، كلاهما يخضع لقواعد وجهات تنظيمية مختلفة، إذ أن هناك جهتي اختصاص مختلفتين للإشراف على الأمن السيبراني وحماية البيانات، ولكل منها شروط مختلفة لمنح التراخيص والغرامات. ثانيا، الفصل بين المسؤوليات يساعد على الحد من تضارب المصالح الذي قد ينشأ عندما يكون المسؤول عن تشغيل الأنظمة هو نفسه المسؤول عن تقييم مدى قانونية استخدام البيانات؛ فعلى سبيل المثال، قد يفضل مسؤول الأمن السيبراني الاحتفاظ بسجلات مفصلة لنشاط العملاء لعدة سنوات للتحقيق في الحوادث، بينما يتعين على مسؤول حماية البيانات التحقق مما إذا كان الاحتفاظ بهذه البيانات الشخصية لهذه المدة ضروريا ومشروعا. ثالثا، تبني الذكاء الاصطناعي يزيد من أهمية حوكمة البيانات، نظرا لاعتماد أدوات الذكاء الاصطناعي على كميات كبيرة من البيانات التي قد تتم معالجتها خارج البلاد.

هل تغيرت النظرة إلى مخاطر الأمن السيبراني في الشرق الأوسط خلال السنوات القليلة الماضية؟

وفقا لتقرير أبرز المخاطر المؤسسية، أدرج 81% من كبار المسؤولين التنفيذيين في مجال التدقيق الداخلي مخاطر الأمن السيبراني ضمن أهم خمس مخاطر في عام 2026، مقابل 72% في عام 2025 و66% في عام 2024. ويوضح الشكل (3) أن المنطقة كانت دون المتوسط العالمي حتى عام 2025، ثم تجاوزته في عام 2026. حيث ظل المتوسط العالمي لمخاطر الأمن السيبراني أعلى منه في الشرق الأوسط حتى عام 2025، إلا أن ذلك تغير في عام 2026، إذ ارتفع تقييم المخاطر في الشرق الأوسط إلى 81%، متجاوزا المتوسط العالمي البالغ 80%. ويرجع ذلك إلى زيادة الاعتماد على التقنيات الرقمية في المنطقة، مما يتيح فرصا أكبر لشن الهجمات السيبرانية، بالإضافة إلى الحرب في الخليج، التي أدت إلى زيادة هذه الهجمات.

الشكل (3): تصنيف مخاطر الأمن السيبراني، 2023-2026
(نسبة الرؤساء التنفيذيين للتدقيق الداخلي الذين اختاروا الأمن السيبراني ضمن أعلى خمسة مخاطر)



المصدر: إعداد المركز المصري للدراسات الاقتصادية، استنادا إلى تقرير أبرز المخاطر المؤسسية، 2027/2026.

وقد لاحظ خبراء الأمن السيبراني في القطاع الخاص هذه الزيادة في المخاطر؛ فوفقا لدراسة CloudSEK، شهدت المنطقة زيادة في نشاط برمجيات الفدية ransomware، إذ ارتفع عدد مصادر معلومات التهديدات التي ترصد هذا النشاط من 17 مصدرا في أبريل 2025 إلى 357 مصدر في يونيو 2026 . كما أفادت شركة ماستركارد Mastercard بأن الهجمات السيبرانية في أوروبا الشرقية والشرق الأوسط وأفريقيا قد ارتفعت بنسبة 13% خلال الفترة ما بين مارس 2025 ومارس 2026، واستحوذ الشرق الأوسط وحده على 49% من إجمالي هذه الزيادة.

ما الذي تفعله الحكومات والقطاع الخاص في الشرق الأوسط؟

استجابت حكومات المنطقة من خلال إنشاء جهات مركزية معنية بالأمن السيبراني ووضع ضوابط ملزمة؛ حيث أنشأت المملكة العربية السعودية الهيئة الوطنية للأمن السيبراني (NCA) عام 2017 لحماية المصالح الحيوية والأمن الوطني والبنية التحتية الحساسة.[4] كما أنشأت دولة الإمارات العربية المتحدة مجلس الأمن السيبراني في عام 2020، واعتمدت الاستراتيجية الوطنية للأمن السيبراني 2025-2031، التي تستند إلى ست ركائز، من بينها الحوكمة، والقدرة الوطنية على الصمود، وأمن التقنيات الناشئة، والشراكات بين القطاعين العام والخاص، وتنمية المواهب.[5] ونتيجة لذلك، جاءت ثمان دول عربية ضمن المستوى الأول (Tier 1) في مؤشر الأمن السيبراني العالمي لعام 2024.[6]

وبرغم هذا التقدم، لا تزال الصورة الإقليمية متفاوتة؛ فقد صُنفت الكويت وتونس والجزائر وليبيا في المستوى الثالث (Tier 3) بينما جاءت العراق ولبنان وسوريا والسودان وفلسطين في المستوى الرابع (Tier 4) ، واليمن في المستوى الخامس (Tier 5).

[4] National Cybersecurity Authority (Saudi Arabia), "About NCA," https://nca.gov.sa/en/vision-and-mission/.
[5] Eventus Security, "UAE National Cybersecurity Strategy 2025-2031."
[6] Telecom Review, "Assessing Arab States in the ITU's GCI 2024."

الجدول (1): تصنيف الدول العربية حسب المستوى في مؤشر الاتحاد الدولي للاتصالات للأمن السيبراني العالمي لعام 2024

المستوى	الدول العربية
المستوى الأول (دول يحتذى بها)	مصر، البحرين، قطر، المغرب، عمان، السعودية، الإمارات
المستوى الثاني (دول متقدمة)	لا يوجد
المستوى الثالث (دول تقوم بإنشاء الأمن السيبراني)	الجزائر، الكويت، ليبيا، تونس
المستوى الرابع (دول ناشئة)	العراق، لبنان، فلسطين، سوريا، السودان
المستوى الخامس (دول تقوم ببناء الأمن السيبراني)	اليمن

المصدر: Global Cybersecurity Index 2024, as reported by Telecom Review[7]

ويشير الاتحاد الدولي للاتصالات إلى وجود فجوة في القدرات السيبرانية في المنطقة، تتسم بمحدودية المهارات والكوادر والمعدات والتمويل. ويرجع ذلك إلى أن الدول ذات التصنيفات الأضعف هي أيضا الأكثر تأثرا بالصراعات والضغوط المالية. وتجدر الإشارة هنا إلى أن المهاجمين يستخدمون الدول ومقدمي الخدمات ذوي الحماية الضعيفة كنقاط دخول إلى الدول الأفضل حماية، مما يحد من فائدة الاستراتيجيات الوطنية التي لا يصاحبها تعاون إقليمي.

جاءت استجابة القطاع الخاص بصورة رئيسية من خلال زيادة الإنفاق وتعزيز إجراءات التحقق والضمان، ومن المتوقع أن يتضاعف الإنفاق على الأمن السيبراني في دول الخليج ليتجاوز 32.7 مليار دولار (120 مليار درهم إماراتي) بحلول عام 2030، مع استحواذ الإمارات والسعودية على أكثر من 60% من إجمالي الإنفاق (Grand View Research, 2025).[8]

ووفقا للتقرير، تعمل المؤسسات المالية على توظيف مزيد من المتخصصين والتعاقد مع المزيد من مقدمي الخدمات لاستيفاء الشروط التنظيمية، وذلك وفقا لما أفاد به كبار المسؤولين التنفيذيين في مجال التدقيق الداخلي خلال حلقات النقاش التي شاركوا فيها. كما غيرت إدارات التدقيق الداخلي أولوياتها، إذ أدرج 78% من كبار المسؤولين التنفيذيين في مجال التدقيق الداخلي في المنطقة الأمن السيبراني ضمن أهم خمسة مجالات ذات أولوية للتدقيق في عام 2026، مقابل 69% في عام 2025، وترتفع هذه النسبة إلى 87% في قطاع الخدمات المالية.[9]

ماذا يجب أن تفعل مصر كي تحمي نفسها من من زايد مخاطر الأمن السيبراني المتزايدة؟

قامت مصر ببناء إطار مؤسسي للأمن السيبراني تدريجيا على مدى العقدين الماضيين؛ حيث أنشأت فريق العمل المصري المعني بالاستعداد لطوارئ الحاسبات (EG-CERT) في عام 2009 تحت مظلة الجهاز القومي لتنظيم الاتصالات (NTRA) ، بهدف الاستجابة لمواجهة الهجمات السيبرانية وتحليلها وإرسال إنذار مبكر للحكومة والجهات المالية وغيرها من قطاعات البنية التحتية المعلوماتية الحيوية. كما أنشأت في عام 2014، المجلس الأعلى للأمن السيبراني (ESCC) والذي تتمثل مهمته في وضع الاستراتيجية الوطنية للاستجابة للتهديدات السيبرانية والإشراف عليها. ثم توسع الإطار القانوني من خلال قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018. وأصدر

[7] Telecom Review, "Assessing Arab States in the ITU's GCI 2024."

[8] Khaleej Times, "Gulf cybersecurity spend to top Dh120 billion by 2030" (19 November 2025), citing Grand View Research. The figure covers the whole Gulf region and is reported in UAE dirhams by the source; converted at the official peg of AED 3.6725 per U.S. dollar.

[9] Internal Audit Foundation and Arab Confederation of Internal Auditors (ARABCIA), Risk in Focus 2026/2027: Hot Topics for Internal Auditors, Middle East (2026). All survey figures in this issue are drawn from this report unless otherwise stated.

المجلس الاستراتيجية الوطنية للأمن السيبراني 2023-2027، والتي تتضمن برامج للتطوير التشريعي، والشراكات الوطنية، والبحث والابتكار، والتوعية المجتمعية، والدفاع السيبراني، والتعاون الدولي.[10]

كما أن القطاع المالي له إجراءات خاصة به يقودها البنك المركزي المصري؛ حيث أنشأ فريق العمل المعني بالاستجابة لحالات الحوسبة المالية في مصر (EG-FinCIRT) the Egypt Financial Computing Incident Response Team لصد الهجمات السيبرانية والتخفيف من آثارها وتبادل المعلومات بين البنوك. وأصبح EG-FinCIRT أول مركز قطاعي في مصر ينضم إلى المنتدى العالمي لفرق الاستجابة للحوادث والأمن (FIRST) في مايو 2023.[11] يتسق هذا النهج القطاعي مع نتائج تقرير أبرز المخاطر المؤسسية، إذ يسجل قطاع الخدمات المالية أعلى تقييم لمخاطر الأمن السيبراني في المنطقة.

وفيما يتعلق بأمن البيانات، طبقت مصر الفصل بين الأمن السيبراني وحماية البيانات، إذ تخضع الأخيرة لقانون منفصل وجهة تنظيمية منفصلة. وصدر قانون حماية البيانات الشخصية رقم 151 لسنة 2020، إلا أن لائحته التنفيذية لم تصدر إلا في نوفمبر 2025 بموجب القرار رقم 816 لسنة 2025، أي بعد أكثر من خمس سنوات من صدور القانون.[12] وتخول اللائحة مركز حماية البيانات الشخصية إصدار تراخيص لمراقبي البيانات والإشراف عليهم، كما تلزم بتعيين مسؤول لحماية البيانات، والإخطار بوقوع الاختراقات خلال 72 ساعة، والحصول على تصريح لنقل البيانات الشخصية عبر الحدود. ومُنحت المؤسسات فترة سماح مدتها عام واحد، ما يعني أنه من المتوقع بدء تطبيق القانون في أواخر عام 2026 وتوقيع غرامات على المخالفات.

ورغم أهمية هذه الإصلاحات، إلا أن التأخر خمس سنوات في إصدار اللائحة التنفيذية للقانون يعتبر مثالا على الفجوة بين التشريع والتنفيذ، ومن المرجح أن تدخل العديد من الشركات فترة تطبيق القانون دون أن تكون لديها خبرة سابقة في الامتثال لمتطلباته.

وبينما ركزت الإجراءات الحكومية على المؤسسات والقوانين، تظهر استجابة القطاع الخاص في حجم الإنفاق والتدريب؛ حيث يقدر حجم سوق الأمن السيبراني في مصر بنحو 257 مليون دولار في عام 2026، ومن المتوقع أن يصل إلى 452 مليون دولار بحلول عام 2031 (Mordor Intelligence، 2026).[13] ويتمثل المحرك الأكبر لهذا النمو في الاستراتيجية الوطنية للأمن السيبراني، التي تسهم في تسريع الإنفاق في القطاع العام. ويستحوذ القطاع المصرفي والخدمات المالية على أكبر حصة من الطلب (31%)، بينما تستحوذ المؤسسات الكبيرة على نحو 68% من الإنفاق. كما استهدفت المبادرات الخاصة تنمية المهارات، ومنها أكاديمية أمن المعلومات التي أطلقها بنك تنمية الصادرات المصري والمعهد المصرفي المصري، وتخصص الأمن السيبراني الذي استحدثته الجامعة الأمريكية بالقاهرة.[14] إلا أنه لا يزال هناك نقص في المتخصصين، إلى جانب تركز الإنفاق في الشركات الكبيرة، يشير إلى أن الشركات الصغيرة والمتوسطة تظل الأقل حماية في مواجهة تهديدات الأمن السيبراني.

[10] Ministry of Communications and Information Technology, "National Cybersecurity Strategy 2023-2027"; Egyptian Supreme Cybersecurity Council; EG-CERT

[11] Egypt Today, "CBE's financial sector cybersecurity center joins global cybersecurity forum" (17 May 2023); Central Bank of Egypt, "EG-FinCIRT acquires the membership of OIC-CERT" (January 2024)

[12] Kennedys, "Egypt's Personal Data Protection Law: the compliance countdown has begun" (2026); Baker McKenzie, "Egypt: Important Data Protection Update" (January 2026).

[13] Mordor Intelligence, "Egypt Cybersecurity Market" (2026).

[14] EnterpriseAM, "The cyber threats facing Egypt and how to address them" (4 December 2024), citing Kaspersky data for H1 2024.

ماذا بعد؟

تشير النتائج بوجه عام إلى أن الأمن السيبراني يشكل أعلى المخاطر التي تواجه المؤسسات على المستوى العالمي وفي الشرق الأوسط، وبالتبعية في مصر، وأدى الصراع الإقليمي وتبني الذكاء الاصطناعي إلى تزايد هذه المخاطر بدلا من أن يحلا محلها. ورغم أن مصر لديها إطار رسمي قوي، وهو ما ينعكس في تصنيفها ضمن **المستوى الأول (Tier 1)**، إلا أن التحدي الرئيسي يكمن في ترجمة هذا الإطار إلى قدرات مطبقة على أرض الواقع. وتلخص النقاط التالية بعض المقترحات في مجال السياسات في هذا الصدد:

- **سد الفجوة بين الالتزام والقدرة على التنفيذ:** يجب أن يمنح المجلس الأعلى للأمن السيبراني الأولوية لتحسين المجالات التي تحقق فيها مصر أدنى مستويات الأداء، وهي إدارة الأزمات السيبرانية وملاحقة الجرائم السيبرانية قضائيا، وذلك من خلال إجراء تدريبات على إدارة الأزمات وإنشاء وحدات متخصصة للتحقيق.
- **التعامل مع الأمن السيبراني وأمن البيانات باعتبارهما مهام منفصلو ولكن يتم التنسيق بينهما:** يجب التنسيق فيما بين كل من المجلس الأعلى للأمن السيبراني، وفريق العمل المصري المعني بالاستعداد لطوارئ الحاسبات (EG-CERT) والبنك المركزي المصري، ومركز حماية البيانات الشخصية فيما يتعلق بشروط الإبلاغ عن الاختراقات، حتى لا تواجه الشركات إجراءات مكررة عندما تكون الواقعة الواحدة هجوما سيبرانيا واختراقا للبيانات الشخصية في نفس الوقت.
- **خفض تكلفة الامتثال على الشركات الأصغر:** يمكن أن يسمح مركز حماية البيانات الشخصية للشركات الصغيرة بالاشتراك في تعيين مسؤول واحد لحماية البيانات، وأن يطبق شروط الامتثال تدريجيا، إذ توضح التجربة السعودية أن إلزام الشركات بتعيين متخصصين منفصلين يرفع التكاليف التي يصعب على الشركات الصغيرة تحملها.
- **زيادة المعروض من المتخصصين:** يجب أن تقوم وزارة الاتصالات وتكنولوجيا المعلومات والجامعات والبنوك بالتوسع في البرامج التدريبية، حيث إن العدد الحالي من الخريجين أقل كثيرا من حجم الطلب في السوق.
- **تعزيز حوكمة المخاطر داخل الشركات:** يجب أن تطلب مجالس الإدارات ولجان المراجعة تقارير دورية عن مستوى نضج إدارة مخاطر الأمن السيبراني، والتعرض للمخاطر المرتبطة بالأطراف الخارجية، واستخدام الذكاء الاصطناعي، إذ إن أقل من نصف المؤسسات في المنطقة تصف حوكمة الأمن السيبراني لديها بأنها ناضجة.
- **تعميق التعاون الإقليمي:** يجب توسيع نطاق تبادل المعلومات بين فرق الاستجابة الوطنية والقطاعية، نظرا لأن الهجمات المرتبطة بجهات حكومية على البنية التحتية الحيوية، إلى جانب تفاوت القدرات بين الدول العربية، يؤديان إلى تعرضهم بشكل للمخاطر.

في النهاية، المسألة ليست بعدد الاستراتيجيات والقوانين الصادرة، وإنما بسرعة واتساق تنفيذها. ويُظهر تأخر صدور اللائحة التنفيذية لقانون حماية البيانات الشخصية في مصر أن بطء التنفيذ يؤدي إلى إطالة فترة عدم اليقين التي تواجهها الشركات. ومن ثم، ينبغي التعامل مع الأمن السيبراني باعتباره جزءا من مناخ الاستثمار والقدرة على الصمود الاقتصادي، وليس مجرد مسألة فنية.