مؤسسة قطر
Qatar Foundation
WISH
مؤتمر القمة العالمي للابتكار في الرعاية الصحية
World Innovation Summit for Health

نوفمبر ٢٠٢٠

حماية نظم الرعاية الصحية

إطار عالمي للأمن السيبراني

نيكي أوبراين
جاي مارتن
إميليا جراس
مايك دوركين
سائرة غافور

صحتنا في عالم واحد

يُستشهد بالتقرير على النحو التالي:
نيكي أوبراين، وجاي مارتن، وإميليا جراس، ومايك دوركين، وسائرة غافور، حماية نظم الرعاية الصحية: إطار عالمي للأمن السيبراني: تقرير شبكة الأنظمة الصحية الرائدة ٢٠٢٠ [تقرير إليكتروني]. معهد الابتكار في مجال الصحة العالمية في إمبريال كوليدج لندن، ٢٠٢٠.

حماية نظم الرعاية الصحية:
إطار عالمي للأمن السيبراني

شبكة الأنظمة الصحية الرائدة ٢٠٢٠

المحتويات

مقدمة

شهد العقد الماضي طفرة في استخدام التكنولوجيات الرقمية الجديدة داخل بيئات الرعاية الصحية كافة، ما أدى إلى إحداث تحسن كبير في إتاحة الوصول إليها وخدمات الرعاية المقدمة فيها. وبفضل هذه التكنولوجيات، أصبح في وسعنا جمع كم هائل من المعلومات ستسهم، بلا شك في صياغة مستقبل جديد للرعاية الصحية وإدخال تحسينات جذرية على النتائج الصحية في جميع أنحاء العالم.

إلا أن ثمة واحد من أبرز التحديات في هذا السياق، ألا وهو كيفية الحفاظ على سلامة هذه البيانات وأمنها بما يضمن استمرار ثقة المرضى والجمهور في مؤسسات الرعاية الصحية التي تحتفظ بمعلومات غاية في السرية عن أنفسهم وعائلاتهم. وليس أيسر من فقدان هذه الثقة عندما نتساهل في حماية الأنظمة الأساسية أو عند ضياع البيانات الشخصية للأفراد.

وشهدت السنوات الخمس الماضية زيادة كبيرة في أعداد الهجمات السيبرانية التي تستهدف مؤسسات الرعاية الصحية. ولا تعد هذه الهجمات مجرد تهديد لأمن المعلومات في سياق الرعاية الصحية، بل إنها تعرض سلامة المرضى أنفسهم للخطر. لذلك، من الأهمية بمكان أن نكون على أهبة الاستعداد وبقدر الإمكان لأي حوادث مستقبلية.

خلال تفشي فيروس كورونا المستجد (كوفيد-١٩)، استغل مجرمو شبكة الإنترنت الخوف والارتباك المنتشران جراء هذه الجائحة، فشهدنا موجة جديدة من الهجمات السيبرانية ضد مؤسسات الرعاية الصحية، بما في ذلك منظمة الصحة العالمية والمراكز الأمريكية لمكافحة الأمراض والوقاية منها. وكشفت الهجمات الكبرى الأخرى، مثل هجوم فيروس الفدية وانا‌كراي على هيئة الخدمات الصحية الوطنية في المملكة المتحدة عام ٢٠١٧، عن مواطن ضعف صارخة داخل الأنظمة الصحية وتأثيرها المحتمل على توفير الرعاية الآمنة للمرضى.

ويحدد هذا التقرير أهم الرؤى في مشهد الأمن السيبراني الدولي للرعاية الصحية ويقترح على مؤسسات الرعاية الصحية إطارًا عالميًا لجاهزية الأمن السيبراني.

ورغم أن ثمة خطوات كبيرة يتعين قطعها في هذا المجال، فإني آمل أن يكون هذا التقرير نقطة انطلاق للأنظمة الصحية تشجعها على تقييم الأمن السيبراني والعمل على تحسينه في نهاية المطاف. ولا غنى عن نشر الوعي والحوكمة والمساءلة في هذا المجال حتى يمكن حماية مؤسسات الرعاية الصحية من الهجمات المستقبلية وضمان توفير خدمات رعاية آمنة لجميع المرضى.

البروفيسور اللورد دارزي من دنهام، OM، KBE، PC، FRS

رئيس مجلس الإدارة التنفيذي لمؤتمر القمة العالمي للابتكار في الرعاية الصحية "ويش"، إحدى مبادرات مؤسسة قطر
المدير المشارك لمعهد الابتكار في مجال الصحة العالمية، إمبريال كوليدج لندن

ملخص تنفيذي

شهدت الأنظمة الصحية تحولًا كبيرًا بفضل التكنولوجيا الرقمية، إذ أسهمت في انخفاض تكاليفها وتحسين إدارة عمليات الرعاية المقدمة للمرضى. إلا أن الانتشار الواسع والكبير لهذه التكنولوجيات الناشئة في مجال الرعاية الصحية لم يسلم من المخاطر الإلكترونية التي تصاحب هذه التكنولوجيات عادة، وهو ما قد يقوض ثقة المرضى في أنظمتهم الصحية ويهدد سلامة بياناتهم وسريتها. ورغم تزايد الهجمات السيبرانية، ما تزال أنظمة الرعاية الصحية ومؤسساتها في جميع أنحاء العالم متخلفة عن الركب من حيث الجاهزية السيبرانية – أي القدرة على مواجهة الهجمات السيبرانية – مقارنة بغيرها من القطاعات. وتجدر الإشارة هنا إلى أن تخطيط الأمن السيبراني ينطوي على تحديات عديدة تواجه الأنظمة الصحية، سواء ذات الدخل المرتفع أو المتوسط أو المنخفض، إذ أن نشر الوعي بأهمية الأمن السيبراني العالمي تنقصه الاستثمارات والدعم المطلوبين.

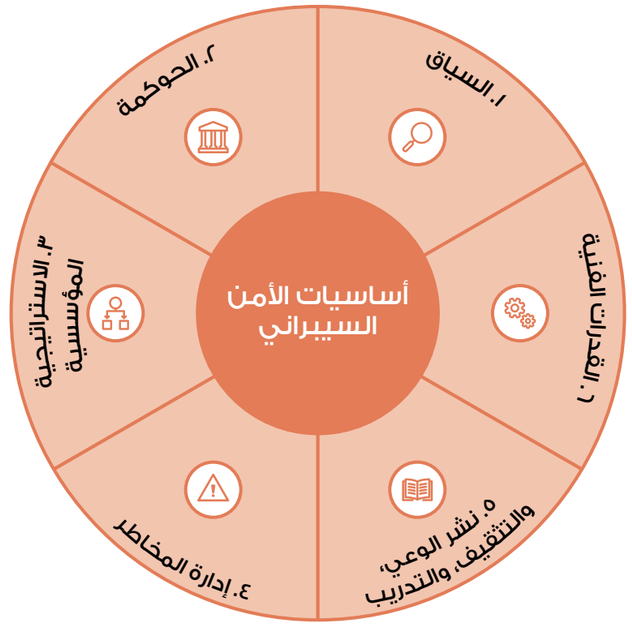
ولا يتوقف الأمر عند هذا الحد، إذ أن الاستثمار وحده لا يضمن النجاح. فها هي الدول ذات الدخل المرتفع خصصت استثمارات لديها من أجل الأمن السيبراني، ومع ذلك فإن نجاحها واجه حجر عثرة تمثل في استخدام نظم معلومات للإدارة الصحية عفى عليها الزمن. ويختلف الأمر بالنسبة للدول ذات الدخل المنخفض والمتوسط، إذ يمكن توجيه هذه الاستثمارات لإنشاء نظام أولي للأمن السيبراني يكون حجر الأساس لمنظومة أكبر وأوسع.

وسنستعرض في هذا التقرير أطر الأمن السيبراني المطبقة حاليًا في مختلف أنحاء العالم، باحثين في الوقت نفسه عن الأسباب التي تجعل من قطاع الرعاية الصحية أحد أضعف المطبقين لأطر الأمن السيبراني.

واستجابةً لحاجة القطاع الملحة لهذه الأطر، استفسرنا من أعضاء شبكة الأنظمة الصحية الرائدة – وهي مجموعة دولية تتألف من نظم صحية ومقدمي خدمات الرعاية الصحية وتنضوي تحت راية معهد الابتكار في مجال الصحة العالمية – وكبار الخبراء في مجالات تكنولوجيا المعلومات والأمن السيبراني والسياسات الصحية والأنظمة الصحية عن خبراتهم وجهودهم التنظيمية المتعلقة بالأمن السيبراني. وأجرينا كذلك استطلاع أولي على أعضاء الشبكة لاستكشاف المشهد العالمي الحالي فيما يخص الأمن السيبراني، أعقبه عقد اجتماع مع مجموعة من الخبراء من مختلف النظم الصحية للإدلاء بأرائهم عن أهم العناصر التي ينبغي أن يضمها أي إطار عالمي للجاهزية السيبرانية في مجال الرعاية الصحية. وتمخض كل ذلك عن وضع إطار عمل يسمى «أساسيات الأمن السيبراني في مؤسسات الرعاية الصحية» بفضل جهد مشترك بين معهد الابتكار في مجال الصحة العالمية وجامعة إمبريال كوليدج لندن بجانب مساهمات شبكة الأنظمة الصحية الرائدة.

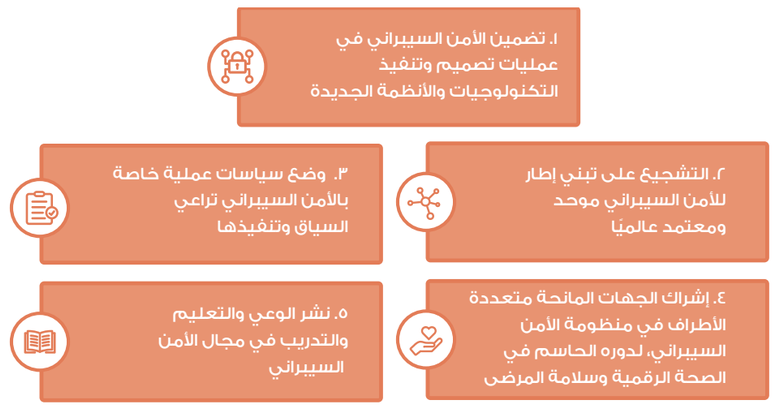
يتضمن إطار الأساسيات هذا أهم عناصر أطر عمل الأمن السيبراني العالمية المخصصة للرعاية الصحية (انظر الشكل ا)، إذ ينص على ستة أبعاد أساسية يلزم مراعاتها عند توسيع نطاق الأمن السيبراني داخل أية مؤسسة من مؤسسات الرعاية الصحية. ويمكن النظر إلى إطار الأساسيات هذا باعتباره «الحد الأدنى المطلوب من المعايير»، أو إطار مرجعي طموح وفقًا لحجم موارد المؤسسة وخبراتها الإلكترونية، أي مدى قدرة المؤسسة على حماية أصولها المعلوماتية من الهجمات السيبرانية. وسنناقش كل بعد من هذه الأبعاد بمزيد من التفصيل في القسم الخامس.

الشكل (١): إطار عمل أساسيات الأمن السيبراني في مؤسسات الرعاية الصحية



لا شك أنه من الصعوبة بمكان إعداد دليل إرشادي عالمي وفعال بشأن الأمن السيبراني، فلا يعد إطار الأساسيات هذا سوى نقطة انطلاق تحتاج إلى مزيد من الخطوات لتعزيز جاهزية الأمن السيبراني مستقبلًا. ويوضح الشكل (٢) هذه الخطوات أو اللبنات الإضافية على النحو التالي.

الشكل (٢): اللبنات الأساسية لتعزيز جاهزية الأمن السيبراني



واخترنا اللبنات الأساسية هذه، الرامية إلى إدخال تحسينات آمنة على استخدام البيانات الصحية وأنظمة سلامة المرضى، لتكون بمنزلة سلسلة توصيات السياسة الخاصة بنا، وذلك على النحو التالي:

١. تضمين الأمن السيبراني في تصميم التكنولوجيات والأنظمة الجديدة وتطبيقها

يلزم على الدول خلال سعيها صوب تعزيز النظم الصحية عبر الرقمنة أن تراعي الأمن السيبراني عند تصميم التكنولوجيات والأنظمة وعند تطبيقها. فعلى المستوى الوطني، يمكن اللجوء إلى إجراءات الحوكمة ووضع اللوائح المناسبة المعنية بالأمن السيبراني داخل قطاع الرعاية الصحية (مثل معايير الأجهزة الطبية) حتى نضمن اتباع أفضل الممارسات على المستوى المحلي. أما على المستوى المؤسسي، فينبغي تكليف مسؤولية الإشراف على الأمن السيبراني للأفراد الذين يتمتعون بحد أدنى من المعرفة بالتهديدات السيبرانية وحلولها.

٢. تعزيز وضع إطار موحد ومعتمد عالميًا للأمن السيبراني

صمم إطار الجاهزية الوارد في هذا التقرير بحيث يمكن استخدامه في مختلف البيئات – أي في الدول ذات الدخل المرتفع والمنخفض والمتوسط على حد سواء – كما روعي أن تكون أولى خطواته هي وضع لغة مشتركة يفهمها الجميع. فعلى المستوى الوطني، ينبغي أن تنطوي أدلة السياسات الاسترشادية رفيعة المستوى على إطار عمل عالمي للأمن السيبراني. بينما على المستوى المؤسسي، فينبغي أن يوجه هذا الإطار عملية وضع خطط الأمن السيبراني واستدامتها. وتأتي هنا الخطوة الثانية، وهي اعتماد هذا الإطار على الصعيد العالمي، الأمر الذي يستلزم معه إبرام شراكات متينة لإجراء البحوث في مختلف المؤسسات بسياقاتها المختلفة ليتسنى لنا في نهاية المطاف الخروج بتوصيات أكثر دقة.

٣. وضع سياسات عملية للأمن السيبراني تراعي السياق، ومن ثمّ تطبيقها

لا بد من مراعاة المخاطر الماثلة وإمكانية التطبيق العملي عند وضع أي إجراءات أو سياسات للأمن السيبراني، بحيث تحد من هذه المخاطر بالشكل المناسب دون الإخلال بتوازن الموارد المطلوبة. ولا بد كذلك أن تحدد الحكومات سلم أولياتها من المهم فالأهم، وتنفيذ التدخلات والأنظمة الفنية البسيطة التي لا تتطلب موارد ضخمة. ويتاح لمختلف المؤسسات حينئذ تقييم التكلفة الاقتصادية لتدخلات الأمن السيبراني بناءً على السياق والموارد المحلية المتاحة.

٤. بناء جسور التواصل مع العديد من الجهات المانحة بشأن الأمن السيبراني لأهمية ذلك المحورية في الصحة الرقمية وسلامة المرضى

لا يمكن تعزيز الجهود على المستوى العالمي دون توفر الموارد المالية والبشرية عند احتياجها، وهو الأمر الذي يزداد أهمية في الدول ذات الدخل المنخفض والمتوسط، إذ أن هذه الدول في حاجة إلى الدعم والمساعدة عند اختيار ممارسات الأمن السيبراني المستدامة وفي بناء خبراتها الفنية. فعلى المستوى الوطني، ينبغي أن تدخل وزارتا الصحة والمالية في نقاش لتحديد الأولويات اللازمة لتطوير القدرات الفنية داخل هيكل إدارتها وإدخال التكنولوجيا الصحية

المناسبة في مؤسسات الرعاية الصحية. وينبغي عليهما كذلك تشجيع الجهات المانحة على مراعاة جوانب الأمن والمرونة وبناء القدرات الفنية في مخصصاتهم المالية. أما على المستوى المؤسسي، فينبغي التركيز على أهمية الأمن السيبراني وتضمينه عند وضع استراتيجية أوسع نطاقًا لتكنولوجيا المعلومات لأنها بمنزلة عامل مساعد للجهود الميدانية المنادية بمراعاة الأمن السيبراني في الاستثمارات الصحية العالمية.

٥. نشر الوعي والتعليم والتدريب في مجال الأمن السيبراني

لا يمكن إغفال ضرورة نشر الوعي بأهمية الأمن السيبراني داخل جميع مستويات الرعاية الصحية – بدءًا من المريض الذي ينبغي إشراكه في المسألة ومرورًا بالعاملين في الخطوط الأمامية الذين عليهم الإلمام بكيفية تضمين النظافة الإلكترونية في مهامهم الوظيفية وانتهاءً بواضعي الخطط والسياسات الصحية ممن ينبغي عليهم إدراك مدى أهمية الأمن السيبراني داخل مؤسساتهم ونظامهم الصحي بوجه عام. فعلى المستوى الوطني، ينبغي اكتساب الخبرة في وضع مناهج دراسية وطنية عن الأمن السيبراني في مجال الرعاية الصحية. أما على المستوى المؤسسي، فينبغي توفير الموارد التعليمية الخاصة بالأمن السيبراني لجميع الموظفين مع العمل على نشر ثقافة الوعي.

القسم الأول: نشر الوعي بالأمن السيبراني في مجال الرعاية الصحية

أدى استخدام التكنولوجيا الرقمية في مجال الرعاية الصحية إلى إحداث تحول كبير في النظم الصحية على مستوى العالم، مما أثمر فوائد ومنافع لا تعد ولا تحصى، من بينها على سبيل المثال: زيادة في تبادل البيانات وتحليلها، واستحداث أساليب إدارة جديدة لرعاية المرضى، وتعزيز إمكانية وصول المرضى للخدمات، كما قللت من تكاليف الخدمات في أغلب الأحيان.[1]

هذا، ويزداد اعتماد النظم الصحية على التكنولوجيات الرقمية يومًا بعد يوم، في الوقت الذي ترسم فيه منظمة الصحة العالمية في استراتيجيتها العالمية بشأن الصحة الرقمية ٢٠٢٠ – ٢٠٢٤ خططها لتسريع وتيرة «إيجاد الحلول المناسبة في مجال الصحة الرقمية واعتمادها للإسراع في اكتشاف سبل استغلال تكنولوجيات الصحة الرقمية في مكافحة تفشي الأوبئة وتطوير البنية التحتية والتطبيقات التي تسمح لنا باستخدام البيانات الصحية في إدارة الأمراض المتفشية». فترسم وثيقة السياسة هذه خطة نضمن بها توسيع نطاق الصحة الرقمية بشكل موثوق به يراعي الجوانب الأخلاقية والسلامة والأمن والإنصاف والاستدامة، ويقوم على المبادئ الأمنية المعنية بالتشغيل والخصوصية والسرية.[2] وحتى يكتب لهذه الاستراتيجية النجاح، لا بد من تأمين النظم الصحية وبياناتها على أن يتم تنفيذها وفق أنظمة أمن ومراقبة مناسبة على يد موظفين مؤهلين تعليميًا. ويتحتم كذلك تبني معايير صارمة في التكنولوجيا المطبقة لضمان تبادل البيانات والوصول إليها.[3]

وعلى الرغم من أننا بدأنا في رصد مزيد من التدفقات الاستثمارية المخصصة لتطبيق الأمن السيبراني في مؤسسات الرعاية الصحية داخل الدول ذات الدخل المرتفع، لا يتم إدخال تحديثات كبيرة على عوامل الأمان في أنظمة معلومات الإدارة الصحية (والتي تكون قديمة في أغلب الأحيان) إلا بعد التعرض لهجوم سيبراني أو أية صورة من صور الخرق الأمني.[4] لذلك، فإن أحد التحديات الكبيرة التي تواجهنا في هذا السياق يتمثل في تنفيذ عمليات للتخطيط الأمني تضمن حماية البيانات والمرضى. بينما نجد في كثير من الدول ذات الدخل المنخفض والمتوسط أن ثمة فرصة «للقفز»* فوق التحديات في الدول ذات الدخل المرتفع وضمان سلامة الأنظمة عند تصميمها – أي أن يكون لديهم أمن سيبراني في أبسط صوره. وفي مثل هذه الظروف، ما تزال الأنظمة الصحية، واستخدام التكنولوجيا الرقمية في مجال الصحة، وأنظمة معلومات الإدارة الصحية في مراحل مبكرة من التطور.

* يعرف المنتدى الاقتصادي العالمي مصطلح «القفز» بأنه وسيلة «لتسريع التنمية وتحقيق نتائج مساوية أو أفضل من نتائج الاقتصادات الناضجة في وقت أقصر».[5]

دأبت الدول ذات الدخل المنخفض والمتوسط في الماضي على استخدام حلول التكنولوجيا الرقمية والصحة الإلكترونية، مثل السجلات الصحية الإلكترونية، لرفع تقارير بالنتائج الصحية للهيئات الدولية أو الجهات المانحة (مثل فيروس نقص المناعة المكتسبة «الإيدز» والسل والملاريا وظهور الأمراض، إلى آخره). ونجد أن السجلات الصحية الإلكترونية بالدول الإفريقية جنوب الصحراء الكبرى حافل بانتهاكات البيانات الشخصية، لا سيما البيانات المتعلقة بمرض الإيدز، الأمر الذي ترتب عليه تداعيات شديدة أو خطيرة على بعض الأفراد. وهو ما يفسر شكوك المجتمعات تجاه سلامة البيانات الصحية واستخدام التكنولوجيا الرقمية في مجال الرعاية الصحية.[6] وليست الصورة قاتمة بالكلية رغم ذلك، فهناك أمثلة أخرى حديثة جرى فيها استخدام التكنولوجيا الرقمية، كأنظمة معلومات الإدارة الصحية، بنجاح على الصعيدين الوطني والمحلي. فشاركت مثلًا وزارة الصحة الرواندية في تطوير نظام للسجلات الطبية الإلكترونية تحتفظ فيه بسجلات المرضى داخل ٣٣ مركز صحي في ثلاث مقاطعات بالبلاد ومنطقة تجمع بشرية تضم ما يربو على ٨٠٠ ألف نسمة.[7]

وبالمثل، يزداد انتشار تكنولوجيا الاتصالات المتنقلة (الخدمات الصحية المتنقلة) داخل أنظمة الرعاية الصحية، لا سيما في الدول ذات الدخل المنخفض والمتوسط.[8] فتعد الأجهزة الجوالة هي الوسيلة الأساسية للوصول إلى شبكة الإنترنت في الدول ذات الدخل المنخفض والمتوسط، مما ساهم في انتشار الخدمات الصحية المتنقلة في هذه البيئات.[9] أما على الصعيد العالمي، فنجد أن النظم الصحية في طريقها للتحول عن الأساليب التقليدية القائمة على استخدام الورق إلى أساليب جديدة آنية يلجأ إليها العاملون في المجال الصحي لتسجيل البيانات الصحية العادية، فيستخدمون الأجهزة الجوالة، مثل الهواتف الذكية أو المساعد الرقمي الشخصي، لجمع البيانات ونقلها وتجميعها داخل مواقع ومستويات متعددة في النظام الصحي. وتكشف لنا البحوث إمكانية حدوث خروقات أمنية عند حفظ المعلومات داخل الأجهزة الجوالة ذات وسائل الحماية الضعيفة أو عند نقل البيانات إلى خوادم مركزية عبر شبكات غير مؤمنة، ناهيك بطبيعة الحال عن فقدان الهواتف أو سرقتها، وهو ما يمثل أحد مصادر القلق الأمني الكبيرة.[10] ومع ذلك، تجدر الإشارة إلى أن ثمة اختلاف بين ابتكارات الصحة الإلكترونية وابتكارات خدمات الصحة المتنقلة، يتطلب معه مراعاة اعتبارات مختلفة عند وضع خطط الأمن السيبراني: إذ يراد بالصحة الإلكترونية خدمات الرعاية الصحية المدعومة بعمليات الإلكترونية بوجه عام، بينما يقصد بالخدمات الصحية المتنقلة تحديدًا حلول الرعاية الصحية التي تتطلب استخدام أجهزة جوالة شخصية.[11]

القسم الثاني: أهمية وضع إطار لجاهزية الأمن السيبراني في مؤسسات الرعاية الصحية

التعريف بالأمن السيبراني وأهم مصطلحاته

يعرف الأمن السيبراني بأنه «آلية الأفراد والمؤسسات للحد من مخاطر الهجمات السيبرانية».[12] ورغم شمولية هذا التعريف نسبيًا وتقديمه شرحًا واسعًا للمفهوم، لا يوجد اتفاق عالمي على تعريف مصطلحاته الأساسية. فعلى سبيل المثال، تعرف وثائق استراتيجية الأمن السيبراني في معظم بلدان العالم «الأمن السيبراني» بأنه الحماية من التهديدات داخل الفضاء الإلكتروني، بينما تقصر فنلندا والنمسا الأمن السيبراني على حماية البنية التحتية الحيوية أو المعلومات الرقمية.[13]

صارت الهجمات السيبرانية أكثر تعقيدًا، بل وقد يتفاقم الوضع بوقوع حوادث إلكترونية واسعة النطاق وعابرة للحدود، مما حدا بالحكومات إلى الاهتمام بشكل أكبر بتعزيز تعاونها الدولي وتكريس الاتفاقات الإقليمية في هذا الشأن.[14,15] وعليه، فإن الوصول لتعريفات واضحة وشاملة ومقبولة دوليًا للأمن السيبراني ومصطلحاته الرئيسة يمثل خطوة مهمة نحو تحقيق هذا الهدف.

مواطن الضعف في قطاع الرعاية الصحية

قد تخلف الجرائم السيبرانية في قطاع الرعاية الصحية تداعيات خطيرة على سلامة المرضى. ومع ذلك، فقد تبين ضعف جاهزية القطاع للجرائم السيبرانية وفق ما ورد رغم أنه أكثر ضعفًا أمامها مقارنة بغيره من القطاعات الحيوية. ويرجع السبب في ذلك إلى عدم وجود ما يضمن توفير التمويل اللازم للأمن السيبراني لا سيما الموجه للنظم الصحية في القطاع العام. ففي المملكة المتحدة مثلًا، لا تنفق كثير من صناديق هيئة الخدمات الصحية الوطنية إلا ١ إلى ٣٪ من ميزانيتها السنوية على البنية التحتية لتكنولوجيا المعلومات، مقارنة بـ ٤ إلى ١٠٪ في القطاعات الأخرى (مثل قطاعي التمويل والاتصالات).[16] (انظر تقرير WISH ٢٠١٨ حول علوم البيانات والذكاء الاصطناعي لمزيد من المعلومات.)

ويزداد الوضع صعوبة في الدول ذات الدخل المنخفض والمتوسط من حيث تمويل الأمن السيبراني في قطاع الرعاية الصحية، حيث تخصص الحكومات نسبة أقل من ناتجها المحلي الإجمالي لصالح قطاع الصحة بأكمله، فلا يتبقى سوى موارد زهيدة تخصص لأمن البيانات وبناء أنظمة صحية سيبرانية متينة. ونجد كذلك في هذه الفئة من الدول أن التبرعات تشكل أكثر من خمس التمويل الذي يتلقاه قطاع الصحة، ويتم توجيه الغالب الأعم من هذه الميزانيات لأمراض أو مبادرات بعينها وليس لترسيخ إدارة النظام الصحي أو بنيته التحتية.[17]

انظر WISH ٢٠١٨ تقرير علوم البيانات والذكاء الاصطناعي، الصفحة ٢٢

الهجمات السيبرانية في مجال الرعاية الصحية

ارتفع عدد الهجمات السيبرانية الموجهة ضد مؤسسات الرعاية الصحية وزادت حدتها بدرجة كبيرة في جميع أنحاء العالم خلال العقد الماضي.[١٨] وثمة هجمات بعينها أسفرت عن تعطيل المؤسسات بشكل كبير، مما أدى إلى تعرضها لخسارات مالية وتعريض سلامة المرضى للخطر (انظر الجدول ١ للاطلاع على قائمة بأحدث الهجمات السيبرانية).

الجدول (١): أحدث الهجمات السيبرانية المتقدمة حول العالم

اسم المنظمة	تاريخ الهجوم	الهدف	أثرها على المرضى
هجوم واناكراي على هيئة الخدمات الصحية الوطنية البريطانية	مايو ٢٠١٧	هيئة الخدمات الصحية الوطنية البريطانية	حظر الوصول للأنظمة، مما منع الموظفين من الوصول إلى بيانات المرضى والخدمات الحيوية. ألغيت آلاف المواعيد والعمليات الجراحية.[١٩]
مجموعة سنغافورة للخدمات الصحية (سنغافورة)	يونيو ٢٠١٨	مجموعة سنغافورة للخدمات الصحية، أكبر مجموعة من مؤسسات الرعاية الصحية في سنغافورة	سرقة البيانات الشخصية لـ ١٫٥ مليون مريض، بما في ذلك الوصفات الطبية لرئيس الوزراء لي هسين لونج.[٢٠]
شبكة مستشفيات ولاية فيكتوريا (أستراليا)	سبتمبر ٢٠١٩	مستشفيات تابعة للتحالف الصحي بمنطقة جيبسلاند، وتحالف الجنوب غربي للصحة الريفية	تأخر أو إلغاء الجراحات وخدمات رعاية المرضى الخارجيين لأن الحادث تتسبب في منع الوصول لعدة أنظمة، بما في ذلك نظام الإدارة المالية.[٢١]
النظام الصحي لمجمع مستشفيات درويد (الولايات المتحدة الأمريكية)	أكتوبر ٢٠١٩	النظام الصحي لمجمع مستشفيات درويد والمراكز الطبية الإقليمية	توقفت رعاية المرضى من ذوي الحالات غير الحرجة لمدة ١٠ أيام. تم دفع مبلغ فدية للمهاجمين لم يكشف عن حجمه لفك شفرة الملفات والسماح باستئناف الخدمات.[٢٢]
مجموعة لايف هيلث كير (جنوب إفريقيا)	يونيو ٢٠٢٠	عمليات تشغيل مجموعة لايف هيلث كير الجنوب إفريقية	أثر الهجوم على أنظمة دخول المرضى ومعالجة الأعمال، بالإضافة إلى خوادم البريد الإلكتروني، مما أدى إلى حدوث تأخيرات إدارية في خدمات المرضى.[٢٣]

الاطار الاول : تحديات الأمن السيبراني في عصر فيروس كورونا المستجد (كوفيد-١٩)

شهدت مؤسسات الرعاية الصحية والاجتماعية والحكومات المحلية تهديدات سيبرانية متزايدة متعلقة بفيروس كورونا المستجد (كوفيد-١٩)، صاحبها زيادة كبيرة في عدد الهجمات خلال هذه الفترة.[٢٤] وتنوع نطاق هذه الهجمات السيبرانية، إذ استهدف المهاجمون الأفراد والمؤسسات على حد سواء في مختلف أنحاء العالم.

وكانت التهديدات الرئيسة للأمن السيبراني خلال فترة فيروس كورونا المستجد (كوفيد-١٩) نتيجة لما يلي:

- التنقلات الكبيرة للموظفين خلال إعادة توزيعهم داخل المؤسسات القائمة أو خارجها للمساعدة في محاربة الجائحة. وأدت هذه التنقلات إلى تخفيف القيود على ضوابط الوصول لأنظمة تكنولوجيا المعلومات، وإلى حدوث أخطاء عرضية بسبب العمل مع أنظمة غير مألوفة.
- تمدد النظم الصحية، صاحبها تطبيق أنظمة تكنولوجيا معلومات جديدة لتجاوز عقبات توفير خدمات الرعاية الصحية للمرضى عن بعد، وأسفر ذلك عن إهمال متابعة المخاطر السيبرانية بصفة يومية
- التطبيق المتسرع لحلول رقمية جديدة دون أن يؤثر ذلك على وصول المرضى لخدمات الرعاية الصحية. وتكتنف هذه التكنولوجيات الجديدة مخاطر عديدة تعرض الأنظمة لمخاطر الاختراق، مثل الثغرات التصميمية التي تهدد أمن البيانات المحفوظة بها.
- عدم وجود رقابة صارمة على عمليات إدخال المحتوى عبر منصات تطبيقات الهواتف الجوالة، مما أدى إلى انتشار المعلومات الخاطئة أو المضللة ويتم تقديمها على أنها إرشادات سريرية غير رسمية.

أظهرت جائحة فيروس كورونا المستجد (كوفيد-١٩) أهمية الأمن السيبراني باعتباره عنصرًا أساسيًا ودائمًا في خدمات الرعاية الصحية، وضرورة اتباع استراتيجيات تخفيف وقائية وتطبيقها. يجب أن تكون في مكانها الصحيح. فالنظم الصحية التي تتمتع بمنظومة أمن سيبراني مرنة تتمتع بالأدوات والخبرات اللازمة لمواجهة التحديات الأخرى التي يتعرض لها أمن المعلومات خلال فترات الأزمات.

التهديدات السيبرانية تهدد سلامة المرضى

يمثل مستوى الأمن السيبراني مصدر قلق كبير فيما يخص سلامة المرضى، إذ أن تعطل البيانات أو تلفها أو تسريبها يؤدي إلى اضطراب كبير في رعاية المرضى وتقويض ثقتهم. فيجب مراعاة المخاطر المرتبطة بتزايد استخدام التكنولوجيا الرقمية في مجال الرعاية الصحية – لا سيما سلامة البيانات الصحية وأمنها – وإدارتها بشكل منهجي في جميع المؤسسات على أن يتم ذلك عبر نهج قابل للتكيف يستجيب للتهديدات الناشئة ويخرج بالدروس المستفادة.(انظر تقرير WISH ٢٠٢٠ حول الصحة العقلية والتقنيات الرقمية وتقرير ٢٠١٨ حول الطب الدقيق لمزيد من المعلومات).

انظر WISH ٢٠٢٠ Mental Health and Digital Technologies Report ، صفحة ٢٨.

انظر تقرير WISH ٢٠١٨ حول الطب الدقيق ، صفحة ١٨.

ومع ذلك، يعجز كثير من قادة النظم والعاملين في قطاع الرعاية الصحية عند إدراك العلاقة بين سلامة المرضى والأمن السيبراني، إذ ينظر لها في الغالب الأعم باعتبارها مشكلة فنية منفصلة. ونتيجة لذلك، ليس في أيدينا كثير من المعلومات عن تأثير ضعف الأمن السيبراني في تقديم رعاية آمنة للمرضى.[٢٥] ومع ذلك، توصل تحليل أجري مؤخرًا على الهجوم السيبراني «واناكراي» الذي استهدف هيئة الخدمات الصحية الوطنية البريطانية إلى أن المستشفيات التي أصيبت مباشرة بفيروس الفدية أفادت: بانخفاض كبير في معدلات دخول حالات الطوارئ والدخول الانتخابي للمرضى، وانخفاضًا يوميًا بنسبة ٦٪ في إجمالي معدل حالات الدخول في كل مستشفى مصابة، وانخفاضًا بنسبة ٤٪ في معدلات دخول حالات الطوارئ، وانخفاضًا بنسبة ٩٪ في معدلات الدخول الانتخابي.[٢٦] ويوضح ذلك أن للهجمات السيبرانية تأثير كبير على إمكانية وصول المرضى لخدمات الرعاية الصحية وتوقيتها المناسب.

في سبتمبر ٢٠٢٠، تم الإبلاغ عن أول حالة وفاة مريض تُعزى مباشرة إلى هجوم إلكتروني؛ تم إرسال امرأة في حالة تهدد حياتها إلى مستشفى على بعد حوالي ٣٠ ميلاً في أعقاب هجوم إلكتروني على مستشفى في دوسلدورف بألمانيا، وتوفيت بعد ذلك بسبب تأخر العلاج.[٢٧]

وفي ظل ذلك التأثير الواضح للهجمات السيبرانية على المرضى – بما في ذلك المخاطر المرتبطة بتأخر معدلات الدخول وإغلاق أقسام الطوارئ أو عدم القدرة على الاطلاع على السجلات الصحية الإلكترونية ونتائج الاختبارات المهمة[٢٨] – فيلزم أن يضع المسؤولون عن توفير الأمن السيبراني في قطاع الرعاية الصحية دوام سلامة المرضى هدفًا واضحًا لهم. ويلزم أيضًا أن يكون الأمن السيبراني نفسه هدفًا واضحًا في عمليات تخطيط سلامة المرضى والاستراتيجيات المنبثقة منها.[٢٩]

ومن الأهمية بمكان فهم عوامل الخطر الكامنة المتعلقة بالأمن السيبراني التي تؤثر على سلامة المرضى وتحييدها، مثل معالجة سوء الإدارة، أو هشاشة الهياكل الأمنية، أو التمويل، أو الثقافات أو السلوكيات التي ترفع من مستوى المخاطر. ومن الضروري أيضًا التعاون مع القيادة وموظفي الخطوط الأمامية لتطبيق نهج وقائي يحمي الأنظمة من الهجمات السيبرانية ويضمن سلامة المرضى. (انظر تقرير WISH ٢٠١٨ حول علوم البيانات والذكاء الاصطناعي وتقرير ٢٠١٥ عن سلامة المرضى لمزيد من المعلومات).

انظر WISH ٢٠١٨ تقرير علوم البيانات والذكاء الاصطناعي، الصفحة ٢٢.

راجع تقرير سلامة المرضى WISH ٢٠١٥، الصفحة ٢١.

القسم الثالث: توسيع نطاق الأمن السيبراني

أطر الأمن السيبراني الحالية

تمثل أطر الأمن السيبراني أدواتًا تعتمدها المؤسسات عامةً لتعزيز المرونة السيبرانية وتحديد الخطوات اللازمة لحماية نفسها.[٣٠] ورغم أن ممارسات الأمن السيبراني الجيدة لا يمكن أن تصل إلى حد الكمال في فعاليتها، تقل احتمالية معاناة المؤسسات الأفضل استعدادًا من الاختراقات، ويرجح معها التعافي السريع من الهجمات بتداعيات أقل من غيرها.

ويهمنا هنا تحديد البيانات والأنظمة التي يجب حمايتها وتعيين أصولها الرئيسة والتأثير المحتمل في حالة تعرضها للاختراق. علاوة على ذلك، يتحتم على المؤسسات تحديد المصادر الاختراق أو الهجوم المحتملة، وأهدافها أو نواياها المحتملة، ومدى قدرتها على تعطيل الأنظمة الأساسية.

في قطاع الأمن السيبراني العالمي، لطالما اعتبرت الولايات المتحدة الأمريكية الرائدة في توفير الأمن السيبراني من خلال NIST Cybersecurity Frame- work، وهو إطار عمل تطوعي للسياسة تم إنشاؤه بالتعاون بين الصناعة والحكومة.[٣١] يستخدم في دول حول العالم. يعتبر توفير الأمن السيبراني أيضًا محور تركيز العديد من الحكومات الوطنية عبر البلدان المرتفعة الدخل، فضلاً عن الهيئات الإقليمية مثل الاتحاد الأوروبي.[٣٢، ٣٣]

في المملكة المتحدة، تم تطوير العديد من أطر الأمن السيبراني لمساعدة المنظمات على تحسين أمنها السيبراني. ومن الأمثلة على ذلك برنامج Cyber Essentials، وهو نظام اعتماد مدعوم من الحكومة ومدعوم من الصناعة. يشتمل التقييم على فحص للثغرات الأمنية، مما يساعد على تحديد البرامج غير المصححة (التعليمات البرمجية المعرضة للخطر) أو البرامج غير المدعومة، والمنافذ المفتوحة، والتكوين غير الصحيح لجدار الحماية، وما إلى ذلك.[٣٤] توفر الشهادة التعلم عن عناصر مختلفة من الأمن السيبراني، على الرغم من أنها لا تطبق هذه المبادئ بشكل مباشر على قطاع الصحة.

مجموعة أدوات أمان وحماية البيانات عبارة عن أداة تقييم ذاتي عبر الإنترنت لمنظمات الرعاية الصحية في المملكة المتحدة لقياس أدائها مقابل معايير الأمان المحددة.[٣٥] يجب على كل مؤسسة لديها إمكانية الوصول إلى بيانات وأنظمة المرضى NHS الامتثال للوائح الحكومية من خلال إكمال التقييم الذاتي.[٣٦]

الاطار ٢ انواع أطر الأمن السيبراني

هناك ثلاثة أنواع شائعة لأطر الأمن السيبراني العامة يجري استخدامها في مختلف القطاعات وفقًا لقدرة المؤسسات واحتياجاتها الأمنية:[٣٧]

أطر التحكم (مثل لائحة المعهد الوطني للمعايير والتكنولوجيا الواردة في نشرتها الخاصة «SP ٨٠٠-٥٣»، وضوابط مركز أمن الإنترنت): تستخدم عادةً من قبل المؤسسات ذات بنية تحتية غير ناضجة نسبيًا في تكنولوجيا المعلومات والإمدادات الأمنية. ويساعد هذا النوع المؤسسات في وضع مجموعة أساسية من الضوابط، والاستفادة من قدراتها التكنولوجية، وتحديد الضوابط الأولى بالتنفيذ، ورسم خارطة طريق مبدئية لفريق الأمن.[٣٨]

أطر قائمة على البرامج (مثل شهادة الأيزو ٢٧٠٠١ التابعة للمنظمة الدولية للتوحيد القياسي، وإطار عمل الأمن السيبراني التابع للمعهد الوطني للمعايير والتكنولوجيا): تستخدم أحيانًا بمصاحبة أطر التحكم لمساعدة المؤسسات في وضع منظومة أمنية أكثر شمولية وفقًا للتقييم الذي يجرى على برامجها القائمة، وفي مقارنة مدى نضج النظام مقارنة بنظائره في الصناعة، وفي تبسيط عمليات التواصل مع قادة الأعمال.[٣٩]

أطر المخاطر (مثل اللوائح ٨٠٠-٣٩، و٨٠٠-٣٧، و٨٠٠-٣٠ التابعة للمعهد الوطني للمعايير والتكنولوجيا، وشهادة الأيزو ٢٧٠٠٥، وتحليل عوامل مخاطر المعلومات «FAIR»): تساعد موظفي الأمن السيبراني في اختيار آلية لتحديد جهود وإجراءات الأمن السيبراني التي تحظى بالأولوية، وفي إدارة البرنامج إدارة تراعي أصحاب المصلحة في مختلف أقسام المؤسسة. ويستعين المتخصصون في مجال الأمن السيبراني بأطر المخاطر لـ: تحديد العمليات الأساسية اللازمة لتقييم المخاطر وإدارتها، وهيكلة برنامج إدارة المخاطر، وتحديد الأنشطة الأمنية ذات الأولوية، وتعيين المخاطر وقياسها وتقدير حجمها.[٤٠]

ومن ناحية أخرى، تقدم الدول ذات الدخل المنخفض والمتوسط هي الأخرى أمثلة ممتازة للريادة الوطنية عندما يتطرق الحديث لتعزيز الأمن السيبراني.[٤١، ٤٢، ٤٣] فاعتمدت كينيا على سبيل المثال نهجًا يتعدد فيه أصحاب المصلحة لتحقيق المرونة السيبرانية. وجاء ذلك بتعاون أبرم بين الحكومة ومؤسسات الاتصالات والمؤسسات المالية والأوساط الأكاديمية وخدمات المرافق العامة ومقدمي البنية التحتية الحيوية، على سبيل المثال لا الحصر.[٤٤] كما أنشأت رواندا الوكالة الوطنية للأمن السيبراني للإشراف على حماية البنية التحتية للمعلومات الحيوية، ووكالة أمن المعلومات الرواندية للإشراف على إدارة البنية التحتية الحكومية، وهيئة تنظيم المرافق في رواندا لمراقبة المؤسسات التشغيلية ومقدمي الخدمات في القطاع الخاص.[٤٥، ٤٦]

أطر الأمن السيبراني في قطاع الرعاية الصحية

يعتبر قطاع الرعاية الصحية على نطاق واسع من أسوأ الجهات المطبقة لأطر الأمن السيبراني، رغم كونه أحد أكثر القطاعات الحيوية المستهدفة. ويمكن لمؤسسات الرعاية الصحية الاستعانة بأطر الأمن السيبراني العالمية الحالية المستخدمة في قطاع الرعاية الصحية للاسترشاد بها في إعداد أطر الأمن السيبراني واختيارها وتطبيقها داخل الهياكل الإدارية الخاصة بها. فعلى سبيل المثال، نشرت الكلية الملكية الأسترالية للممارسين العامين مجموعة من المعايير لمؤسسات وشركات قطاع الرعاية الصحية، تتضمن توجيهات بشأن عمليات تخطيط التعافي من الهجمات وإدارة الوصول للخدمات وتقييم المخاطر.[٤٧]

ومع ذلك، ما نزال نفتقد لمعايير دولية توضع خصيصًا لقطاع الرعاية الصحية. فبالنسبة للدول ذات الدخل المرتفع، فإن التحديات والعوائق التي تحول بينها وبين تنفيذ معايير متسقة للأمن السيبراني في مختلف مؤسساتها تشمل ما يلي:

- الإدارة المجزأة
- حاجة المستخدمين للاطلاع على سجلات المرضى في أي وقت
- عدم إقدام القيادات على الضغط من أجل تحسين معايير الأمن والترابط
- محدودية الموارد اللازمة للإنفاق على حلول الأمن السيبراني، بما في ذلك الخبرات المهنية.[٤٨]

وبالنسبة لدول الخليج، فإن دولة الإمارات العربية المتحدة والمملكة العربية السعودية هما الوحيدتان اللتان تطبقان لوائح أمن سيبراني مخصصة للرعاية الصحية. وفي ظل غياب مثل هذه اللوائح فإن الدول تواجه صعوبة في إنشاء الهيكل الإداري اللازم لتعزيز مرونتها خلال مواجهة تحديات الأمن السيبراني.[٤٩] ولا يختلف الأمر كثيرًا في الدول ذات الدخل المنخفض والمتوسط، فنجد فيها كثيرًا من التحديات نفسها، ولكنها في الوقت نفسه تواجه عوائق أخرى يجب وضعها في الاعتبار، من بينها ضعف الوعي العام بتهديدات الأمن السيبراني، والافتقار إلى لغة مشتركة وبنية تحتية لتكنولوجيا المعلومات، وضعف الموارد المالية اللازمة لتعزيز مرونة الأمن السيبراني في القطاع الصحي.[٥٠، ٥١، ٥٢]

وما يزال من الصعب ترجمة الجهود التي تبذل على المستوى الوطني لتحقيق الأمن السيبراني إلى أدلة استرشادية وإجراءات هادفة داخل قطاع الرعاية الصحية. ومع ذلك، لا مفر من استكشاف حالة الأمن السيبراني في مختلف بيئات الرعاية الصحية الدولية، للوصول إلى إطار عالمي للجاهزية يتيح لنا رسم خطط الأمن السيبراني في مختلف النظم الصحية والمؤسسات الفردية.

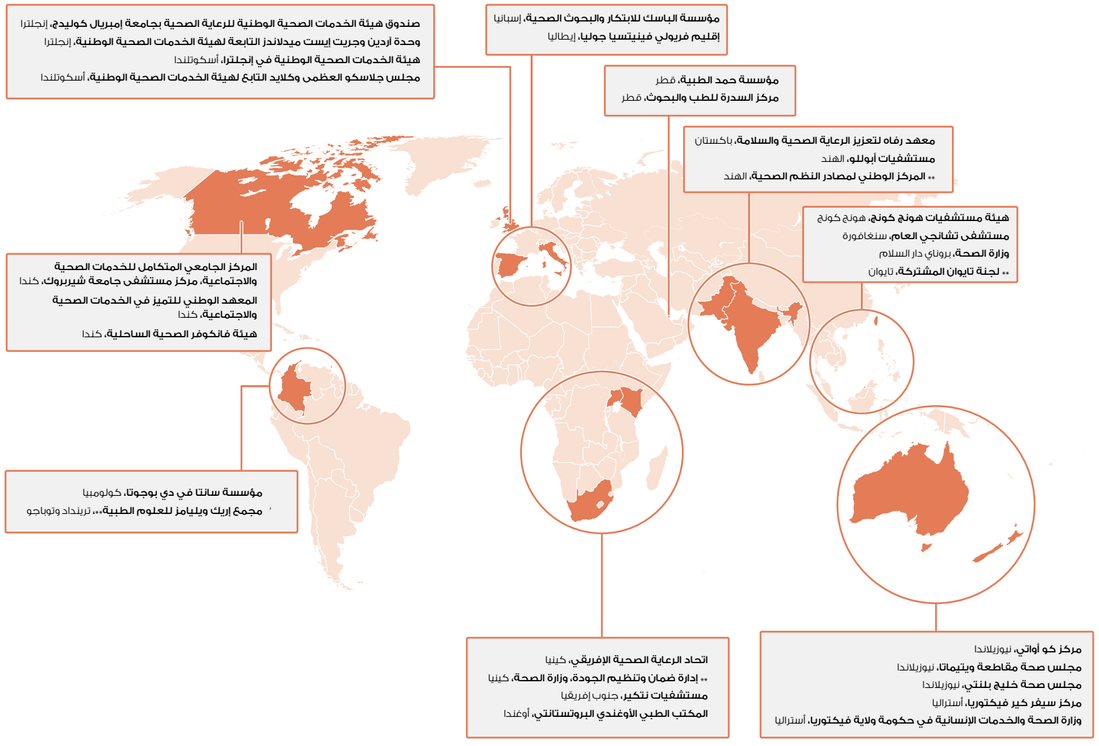
القسم الرابع: تعرض أعضاء شبكة الأنظمة الصحية الرائدة للهجمات السيبرانية وآلية تطويرهم للأمن السيبراني

يقدم هذا القسم نظرة عامة على تجارب المؤسسات الأعضاء في شبكة الأنظمة الصحية الرائدة والجهود المؤسسية المعنية بالأمن السيبراني.

نظرة عامة على شبكة الأنظمة الصحية الرائدة

تتخذ شبكة الأنظمة الصحية الرائدة من معهد الابتكار الصحي العالمي في جامعة إمبريال كوليدج لندن مقرًا لها، وهي شبكة تعاونية تتألف من رواد الرعاية الصحية ومؤسساتها التي كرست نفسها من أجل تحسين عمليات تقديم الرعاية الصحية. وتمثل الشبكة حلقة وصل بين قادة ومؤسسات الرعاية الصحية التي تثمن التبادل الدولي للأدلة وأفضل الممارسات. وتساعد الشبكة في عمليات جمع البيانات وتوثيق التعاون بين المؤسسات الصحية وتبادل المعرفة فيما بينها بأساليب تعود بقيمة مضافة على أنظمة الرعاية الصحية على الأصعدة الدولية والوطنية والمحلية.

الشكل (٣): خريطة عضوية شبكة الأنظمة الصحية الرائدة



المصدر: www.leadinghealthsystemsnetwork.org/members

نهج مشروع الأمن السيبراني

أجري مشروع شبكة الأنظمة الصحية الرائدة للأمن السيبراني على جزئين:

الجزء الأول (الاستطلاع): سعى الجزء الأول إلى استكشاف المشهد العالمي الحالي للأمن السيبراني من خلال إجراء استطلاع على تجارب المؤسسات الأعضاء في شبكة الأنظمة الصحية الرائدة في مختلف أنحاء العالم. وتضم الشبكة عددًا من المؤسسات العالمية التي تتخذ من قطاع الصحة محورًا لها، مما يمنحنا نظرة عريضة على وضع الأمن السيبراني في هذا القطاع.

تضمن الاستطلاع قسمين رئيسين:

- **المشهد المؤسسي للأمن السيبراني:** تضمن أسئلة تهدف إلى تقييم تجربة كل مؤسسة مع الهجمات السيبرانية وعمليات تخطيطها للأمن السيبراني.

- **مستوى نضج الأمن السيبراني:** تم إعداد هذا القسم وفقًا لنموذج نضج قدرات الأمن السيبراني لدى الدول الذي أعده المركز العالمي لقدرات الأمن السيبراني،[٣٥] وشهد طرح أسئلة حول مستوى تخطيط المؤسسات في مجالات الأمن السيبراني الستة لتحديد مستوى نضج استجابتها. وبعد تجميع بيانات الإجابات وتحليلها، استخدم الفريق البحثي النتائج لاستكمال الجزء الثاني من المشروع.

الجزء الثاني (تقنية دلفي لتحقيق التوافق في الآراء): جمع الجزء الثاني من المشروع مجموعة من الخبراء في مجالات الأمن السيبراني وتكنولوجيا المعلومات والمعلوماتية الصحية تابعين لأنظمة صحية مختلفة، وذلك بغية الوقوف على أهم العناصر المرتبطة بإطار أمن سيبراني عالمي للرعاية الصحية

أجريت تقنية دلفي بشكل إليكتروني، وشارك فيها ٣٤ خبيرًا من ١٦ دولة. وتستعين التقنية بوسائل التواصل المنظمة والبحث المنهجي، فتعتمد على فريق الخبراء للتوصل إلى إجماع بشأن موضوعات بعينها. ويجيب الخبراء على استبيانات للرأي في جولات متتابعة، ويقوم المشرف بعد ذلك بتقديم ملخص عن حكم الخبراء عقب كل جولة دون ذكر الأسماء. ويتاح للمشاركين إعادة النظر في إجاباتهم السابقة في ضوء المعلومات التي حصلوا عليها مع بداية كل جولة. وفي نهاية المطاف، تتوقف العملية بعد استيفاء شرط محدد مسبقًا (مثل الوصول لعدد محدد سلفًا من الجولات أو التوصل إلى إجماع).[٣٤]

وقام الخبراء خلال الجزء الثاني من المشروع بالإجابة على الاستبيانات في ثلاث جولات. وكانت الغاية الوصول إلى اتفاق في الآراء حول أهم الموضوعات أو المكونات اللازمة لوضع إطار جاهزية عالمية للأمن السيبراني في قطاع الرعاية الصحية، وهو ما تحقق فعلًا في نهاية الجولة الثالثة.

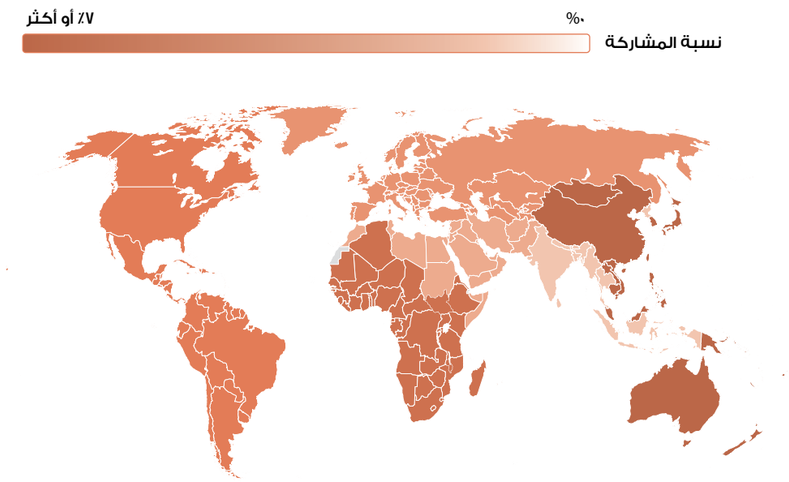
نتائج مشروع الأمن السيبراني لشبكة الأنظمة الصحية الرائدة

نتائج الجزء الأول (الاستطلاع)

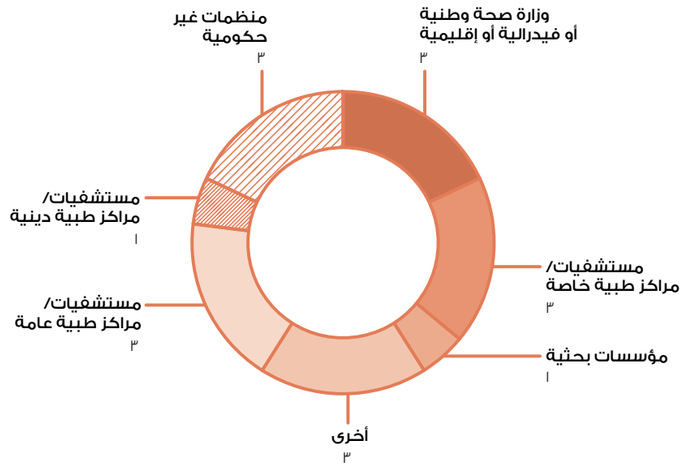
شاركت ١٧ مؤسسة في الاستطلاع موزعة على ست مناطق جغرافية (انظر الشكل ٤). وشكلت المستشفيات/ المراكز الطبية العامة ١٧،٦٥٪ منها، والدينية ٥،٨٪، والخاصة ١٧،٦٥٪، ووزارات الصحة الإقليمية ١٧،٦٥٪، والمنظمات غير الحكومة ١٧،٦٥٪، والمؤسسات البحثية ٥،٨٨٪، بينما صنف الباقي كأخرى وكانت نسبته ١٧،٦٥٪ (انظر الشكل ٥).

وأفادت جميع مؤسسات الرعاية الصحية أنه سبق لها استخدام السجلات الصحية الإلكترونية إلى حد ما، رغم التنوع في مستويات النضج الرقمي فيما بينها.

الشكل (٤): المشاركة حسب المنطقة كما حددتها منظمة الصحة العالمية (العدد = ١٧)



الشكل (٥): المشاركة حسب القطاع (العدد = ١٧)



١. مواقف المشاركين تجاه الأمن السيبراني

سُئل المشاركون في الاستطلاع عما يعدونه أكبر تهديد للأمن السيبراني داخل مؤسساتهم.

- رأى أغلب المشاركين أن أكبر تهديد للأمن السيبراني يتعلق بالبيانات، إذ أشاروا إلى أن من أكبر مخاوفهم هو احتمالية فقدان السجلات الصحية أو التلاعب بها، حيث يمكن استغلال هذه البيانات في عمليات الابتزاز أو الاحتيال على الأفراد أو المؤسسات، وهو ما قد يفضي إلى فقدان الثقة في مؤسسات الرعاية الصحية وإلحاق الضرر بسمعتها.

- أشار العديد من المشاركين أيضًا إلى مخاطر تعطل الخدمات باعتبارها تهديدًا رئيسًا للأمن السيبراني ومرونة التعامل مع التهديدات. كشف آخرون عن مخاوفهم تجاه التبعات المترتبة على تعطل الخدمات، لا سيما ما قد يلحق بالمرضى من ضرر أو وفاتهم، أو الانعكاسات المالية على المرضى والمؤسسة نفسها.

- وبالمثل، كانت المخاطر المتعلقة بإدارة المؤسسة أحد المخاوف لدى الكثيرين.كانت التهديدات الداخلية أو الداخلية مثل التسريب المتعمد أو غير المتعمد للبيانات والهجمات السيبرانية التي تؤثر على العمليات (وتحديدًا قدرة المؤسسة على تقديم خدمات رعاية المرضى) هي التداعيات الرئيسة التي رأى المشاركون أنها تنتج عن سوء الإدارة.

- تمثل آخر التهديدات التي سجلها المشاركون في الجانب التكنولوجي، إذ عبروا عن مخاوفهم تجاه مواطن الضعف داخل النظام وفيروسات الفدية. ومع ذلك، نجد أنهم عبروا أيضًا عن مخاوف ينفرد بها قطاع الصحة، وهو التهديدات التي تفرضها أتمتة الخدمات الطبية والخدمات ذات الصلة، ومواجهة أي اضطرابات في الخدمة تفضي إلى حدوث وفيات بين المرضى، وتقادم أنظمة المعلومات والمعدات الطبية الحيوية وتنوعها.

٢. التجارب مع الهجمات السيبرانية

- رصدنا في العينة تزايد الهجمات السيبرانية في جميع المؤسسات على مدار العامين الماضيين. تعرض ٥٦٪ من المؤسسات لهجوم سيبراني خلال الأشهر الـ ١٢ الماضية (انظر الشكل ٦)، رغم أن البعض منها لم يكن على علم بوقوع هذه الهجمات السيبرانية.

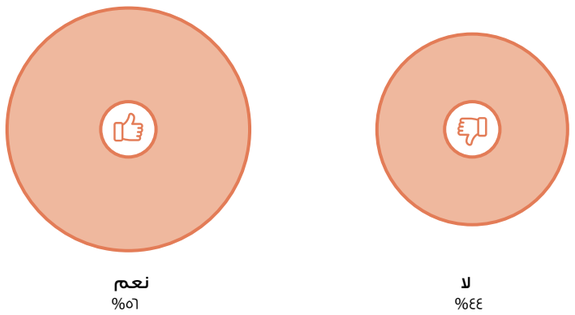
- ذكر المشاركون في الاستطلاع عددًا من تداعيات الهجمات السيبرانية، من بينها تعطل نظام العمل، وفقدان البيانات، وإلغاء مواعيد المرضى، وتأخير المشاريع، بجانب تكاليف الفرص البديلة لهذه التداعيات. وتجدر الإشارة هنا إلى أن بعض المؤسسات لم تكن دراية بحجم هذه الهجمات كاملًا.

- أبدى المشاركون ردودًا إيجابية بوجه عام تجاه مدى فعاليتهم في التعامل مع الهجمات السيبرانية التي وقعت خلال الأشهر الـ ١٢ الماضية.بلغ متوسط الدرجات التي أعطاها المشاركون لفعالية الأمن السيبراني في مؤسساتهم ٧ من ١٠ درجات (العدد = ١٦). ومع ذلك، منح ٣٧٪ من المشاركين ٦ درجات أو أقل لمؤسساتهم.

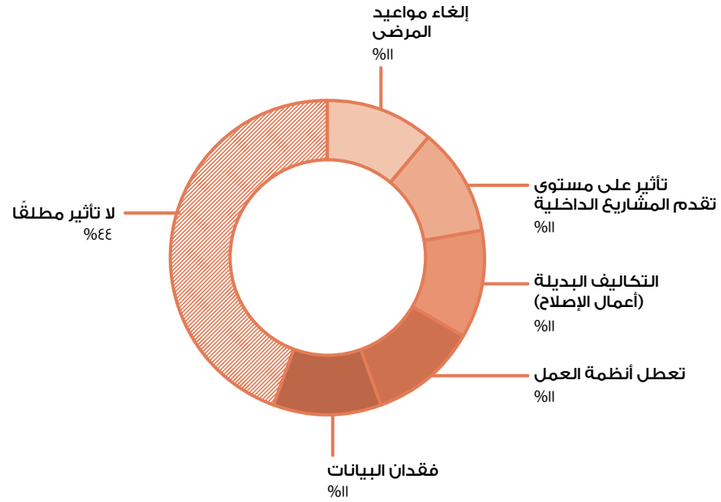
- تمثل آخر التهديدات التي سجلها المشاركون في الجانب التكنولوجي، إذ عبروا عن مخاوفهم تجاه مواطن الضعف داخل النظام وفيروسات الفدية. ومع ذلك، نجد أنهم عبروا أيضًا عن مخاوف ينفرد بها قطاع الصحة، وهو التهديدات التي تفرضها أتمتة الخدمات الطبية والخدمات ذات الصلة، ومواجهة أي اضطرابات في الخدمة تفضي إلى حدوث وفيات بين المرضى، وتقادم أنظمة المعلومات والمعدات الطبية الحيوية وتنوعها.

الشكل (٦): تجارب الهجمات السيبرانية خلال الأشهر الـ ١٢ الماضية (العدد = ١٦)

هل تعرضت مؤسستك لهجوم سيبراني خلال الـ ١٢ شهرًا الماضية؟



الشكل (٧): التأثير المسجل لأخطر الهجمات السيبرانية المبلغ عنها (العدد = ٩)



٣. إدارة الأمن السيبراني

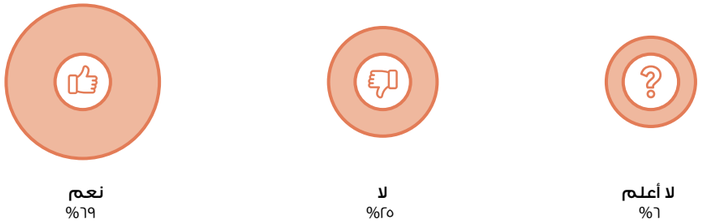
- طُلب من غالبية المشاركين (العدد = ١٦) الإبلاغ عن الحوادث السيبرانية التزامًا بالمتطلبات التنظيمية أو القانونية المحلية أو الوطنية (٦٩٪) (انظر الشكل ٨).

- من بين أولئك الذين طُلب منهم الإبلاغ عن هذه الحوادث، لجأ ٧٣٪ إلى رفع تقارير داخلية للقيادة العليا/ مجلس الإدارة (بما في ذلك كبير مسؤولي أمن المعلومات أو كبير مسؤولي المعلومات)، ولجأ ٥٥٪ منهم إلى رفع تقاريرهم إلى إحدى هيئات حماية البيانات الوطنية، ولجأ ٣٦٪ منهم إلى رفع تقاريرهم إلى وزارة الصحة.

- وجدنا أن أغلب الذين أجابوا بأنهم غير ملزمين بالإبلاغ عن الحوادث السيبرانية وفق متطلبات وطنية تنظيمية أو قانونية يعملون في بيئات صحية ذات دخل منخفض أو متوسط، ويصنف نصفهم ضمن المنظمات غير الربحية/ غير الحكومية.

الشكل (٨): المتطلبات التنظيمية للأمن السيبراني (العدد = ١٦)

هل يجب على مؤسستك الإبلاغ عن الحوادث السيبرانية التزامًا أي متطلبات تنظيمية/ قانونية محلية أو وطنية؟



- وجدنا في العينة أن الغالبية العظمى (٩٤٪) أفادت بأن الأمن السيبراني يشكل جزءًا في جدول أعمال قيادة المؤسسة أو مجلس إدارتها (انظر الشكل ٩).

- أفاد ٦٢٪ فقط بتوفر البرامج التدريبية لقيادة المؤسسة (انظر الشكل ١٠).

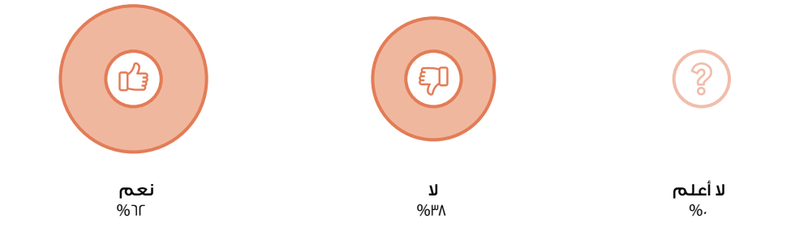
- أفاد ٦٠٪ بأن أحد أعضاء مجلس الإدارة جرى تعيينه قائدًا/ مسؤولًا عن الأمن السيبراني (انظر الشكل ١١).

- لم يسبق لغالبية المؤسسات (٧٥٪) بإجراء محاكاة للهجمات السيبرانية الخطيرة (انظر الشكل ١٢).

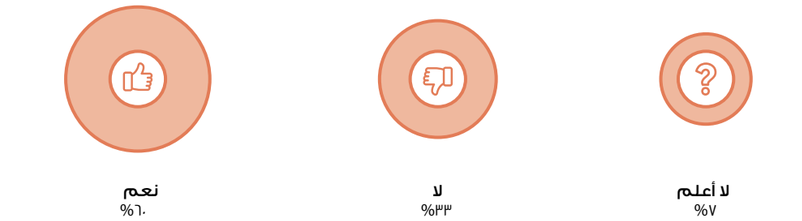
الشكل ٩: الأمن السيبراني وجدول أعمال القيادة المؤسسية (العدد = ١٦)

هل الأمن السيبراني يشكل جزءًا من جدول أعمال قيادة/ مجلس إدارة مؤسستك؟

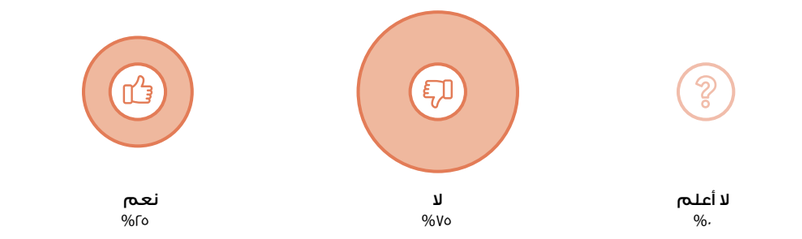
الشكل ١٠: التدريب على الأمن السيبراني لقادة المؤسسات (العدد = ١٣)



الشكل ١١: الأمن السيبراني ومسؤولية القيادة المؤسسية (العدد = ١٥)



الشكل ١٢: محاكاة المؤسسات للهجمات السيبرانية (العدد = ١٢)

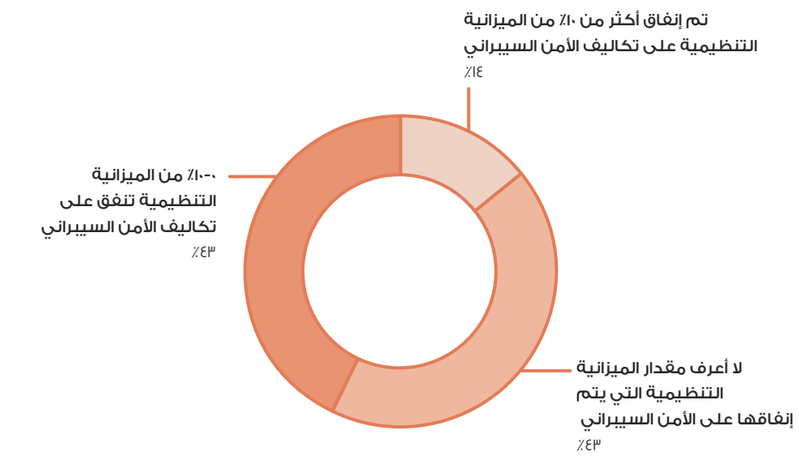


٢. الإدارة المالية

وجه سؤال للمشاركين في الاستطلاع (عدد = ١٦) يتعلق بوجه خاص بالإدارة المالية داخل مؤسساتهم.

- وتراوحت النسبة المئوية المقتطعة للأمن السيبراني من ميزانية المؤسسة بين ٠ إلى ١٠٪ (٤٣٪) وبين ١٦ إلى ٧٠٪ (٧٪) (انظر الشكل ١٣).
- .وتراوحت النسبة المئوية المقتطعة للأمن السيبراني من ميزانية المؤسسة بين ٠ إلى ١٠٪ (٤٣٪) وبين ١٦ إلى ٧٠٪ (٧٪) (انظر الشكل ١٣).
- أنفق غالبية المشاركين ما تعادل نسبته ٠ إلى ١٠٪ من ميزانية المؤسسة على الأمن السيبراني. وربما يرجع هذا الاختلاف الكبير في النسب المسجلة إلى اختلاف مؤسسات الرعاية الصحية المشاركة في الاستطلاع، أو اختلافهم في تفسير المراد من «ميزانية المؤسسة».
- قد يرجع نطاق النسب المئوية المبلغ عنها إلى أنواع مختلفة من مؤسسات الرعاية الصحية التي شاركت في الاستطلاع ، أو تفسيرات مختلفة لـ «الميزانية التنظيمية».
- لم يعلم ٤٣٪ من المشاركين النسبة المئوية المقتطعة للأمن السيبراني من ميزانية المؤسسة. ومع ذلك، أفاد ٧١٪ من المشاركين بأن ميزانية الأمن السيبراني قد زادت في الأشهر الـ ١٢ الماضية (انظر الشكل ١٤).

الشكل ١٣: النسبة المئوية المقتطعة لتكاليف الأمن السيبراني في ميزانية المؤسسة (العدد = ١٤)



٥. قياس النضج السيبراني

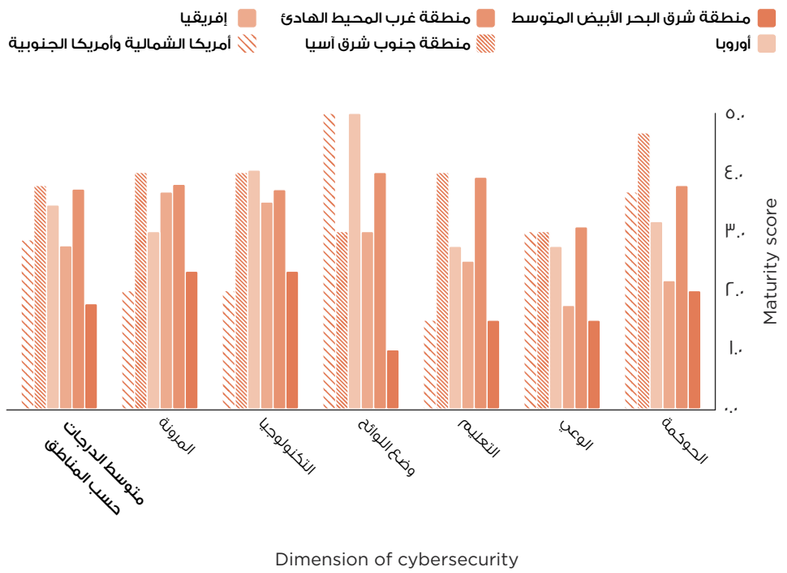
وضعت الأسئلة الخاصة بهذا القسم وفق أبعاد ومستويات النضج الموضحة في نموذج نضج قدرات الأمن السيبراني لدى الدول الذي أعده المركز العالمي لقدرات الأمن السيبراني لتقييم النضج السيبراني لدى المؤسسات.[٥٥]

ويحدد النموذج خمسة أبعاد تغطي مختلف جوانب الأمن السيبراني، ويتم من خلالها تحديد المجالات التي يجب أخذها في الاعتبار عند السعي إلى تطوير القدرات.[٥٦] وتصف مستويات النضج ما أحرزته دولة ما من تقدم في جوانب معينة من أبعاد الأمن السيبراني. وتمر المؤسسات بخمسة مراحل لتحقيق النضج، هي على النحو التالي: الانطلاقة ثم التكوين ثم التأسيس، تليها المرحلة الاستراتيجية ثم المرحلة الديناميكية. وجرى اختيار أبعاد مستويات النضج الموضحة في النموذج لتكون انطلاقة نستهل بها الاستطلاع، لا سيما وأنها تحظى بالموثوقية في جميع المجالات، وليس قطاع الرعاية الصحية فحسب.

وخلال رسم مسار الاستطلاع وتصميمه، حدد الفريق البحثي جوانب الأمن السيبراني التي يريد تناولها انطلاقًا من ستة أبعاد وليس خمسة، ليعبر بشكل أفضل عن مستوى النضج في قطاع الرعاية الصحية على وجه الخصوص وقياسه بدقة أفضل، وانطلاقًا من الصعيد المؤسسي وليس الصعيد الوطني.[٥٧] وطرحت أسئلة تتناول المجالات الستة على المشاركين، وهي: الحوكمة (التخطيط للهجمات السيبرانية وتعزيز الأمن السيبراني)، والوعي (المعرفة المؤسسية بالتهديدات والحوادث السيبرانية وسبل التصدي لها بشكل مناسب)، والتعليم (تدريب أصحاب المصلحة داخل المؤسسة على الأمن السيبراني)، ووضع اللوائح (المتطلبات التشريعية الوطنية المعنية بالأمن السيبراني)، والتكنولوجيا (أمن التكنولوجيا والبنية التحتية لتكنولوجيا المعلومات داخل المؤسسة)، والمرونة (قدرة المؤسسة على الاستجابة للتهديدات والهجمات السيبرانية).

وتم تصنيف الإجابات حسب مقياس للنضج بحيث من يحرز نقطة واحدة يصنف ضمن مرحلة الانطلاقة، ومن يحرز نقطتين يصنف ضمن مرحلة التكوين، ومن يحرز ثلاث نقاط يصنف ضمن مرحلة التأسيس، ومن يحرز أربع نقاط يصنف ضمن المرحلة الاستراتيجية، ومن يحرز خمس نقاط يصنف ضمن المرحلة الديناميكية.[٥٨] ويوضح الشكل (١٤) متوسط النقاط لكل بعد ومنطقة.

الشكل (١٤): درجات النضج السيبراني حسب الأبعاد/ المناطق (العدد = ١٣)



الجدول (٣): تصنيف النضج السيبراني حسب المناطق (العدد = ١٣)

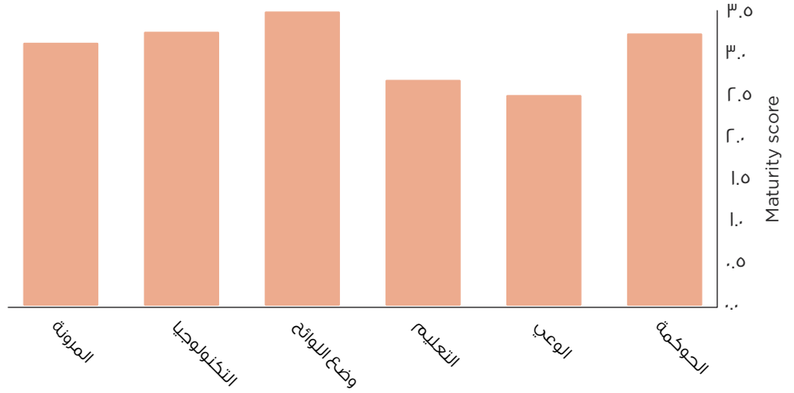
المنطقة	درجة النضج	التصنيف
إفريقيا	٢.٧	مرحلة التأسيس
شرق البحر الأبيض المتوسط	١.٧	مرحلة التكوين
أوروبا	٣.٤	مرحلة التأسيس
أمريكا الشمالية وأمريكا الجنوبية	٢.٨	مرحلة التأسيس
جنوب شرق آسيا	٣.٧	المرحلة الاستراتيجية
غرب المحيط الهادئ	٣.٧	المرحلة الاستراتيجية

كشفت الدرجات الإقليمية عن مجالات معينة تتمتع فيها المؤسسات المشاركة بمستويات بعينها من النضج وأخرى تحتاج إلى مزيد من التحسين. فنجد أن درجات أوروبا وأمريكا الشمالية وأمريكا الجنوبية عالية بوجه خاص في ناحية وضع اللوائح، بينما سجلت منطقتا شرق البحر الأبيض المتوسط وجنوب شرق آسيا نقاط ضعيفة نسبيًا فيها. وعلى الجانب المقابل، نجد أن نقاط منطقة جنوب شرق آسيا عالية بوجه خاص في مجال الحوكمة مثلها في ذلك مثل منطقة غرب المحيط الهادئ. وأحرزت إفريقيا أعلى النقاط في التكنولوجيا والمرونة بينما حصلت على أدناها في كل من التعليم والوعي. كما حققت أمريكا الشمالية وأمريكا الجنوبية أقل النقاط في التعليم.

وعند حساب متوسط النقاط في جميع المجالات، نجد أن منطقة جنوب شرق آسيا حققت أعلى مستوى نضج حيث حصلت على معدل نقاط يبلغ (٣.٧) مما يضعها في تصنيف المرحلة الاستراتيجية

(انظر الجدول ٢). وصنفت منطقة غرب المحيط الهادئ ضمن المرحلة نفسها لتحقيقها متوسط نقاط يبلغ (٣،٧). وتجدر الإشارة إلى أن مؤسسات هاتين المنطقتين شهدتا مبالغات في عدد الهجمات السيبرانية التي تعرضت لها خلال الـ ١٢ شهر السابقة، حيث سجلت هاتان المنطقتان أقل عدد من الهجمات مقارنة بالهجمات التي سجلتها المناطق الأخرى (عددها = ٨). هذا، وصنفت ثلاث مناطق ضمن مرحلة التأسيس وفقًا لما حققته من نقاط: فنجد أن أوروبا حققت متوسط نقاط يبلغ (٣،٤)، وحققت أمريكا الشمالية وأمريكا الجنوبية متوسط نقاط يبلغ (٢،٨)، وحققت إفريقيا متوسط نقاط يبلغ (٢،٧). وصنفت منطقة شرق البحر الأبيض المتوسط ضمن مرحلة التكوين وفق متوسط النقاط الذي أحرزته والبالغ (١،٧).

ونجد كذلك أن البعد الذي حقق أعلى نقاط في مستوى النضج هو بعد وضع اللوائح (٣،٥) (انظر الشكل ١٦). وبالنسبة للأبعاد الأخرى التي أحرزت نقاط أعلى من ٣ نقاط (أي تندرج تحت مرحلة التأسيس)، فكانت الحوكمة (٣،٢)، والتكنولوجيا: البنية التحتية للخدمات (٣،٢)، والمرونة (٣،١). وعلى الجانب الآخر، نجد أن بعدي الوعي (٢،٥) والتعليم (٢،٦) لم يحققا ثلاث نقاط مما يشير إلى أنها المجالات الأقل تطورًا داخل المؤسسات المشاركة في الاستطلاع.



الشكل (١٥): نقاط النضج السيبراني حسب الأبعاد (العدد = ١٣)

ملخص نتائج الاستطلاع

أظهر هذا الاستطلاع أن التهديدات السيبرانية تشكل مصدر قلق بالغ لمؤسسات الرعاية الصحية على مستوى العالم. وكانت البيانات هي أكثر المخاطر إثارة للمخاوف عند التطرق للحديث عن الأمن السيبراني، إذ أشار المشاركون إلى اعتمادهم على السجلات الصحية الإلكترونية ومخاوفهم من فقدان هذه السجلات أو التلاعب بها. وسلطت تقارير الهجمات الحالية الضوء على التأثير بعيد المدى للهجمات السيبرانية على المرضى والمؤسسات، وليس أقلها التأخير في توفير خدمات الرعاية الصحية.

وكشفت النتائج كذلك عن اهتمام عالمي بتوفير قدر ما من التدريب على بعدي الحوكمة والوعي في الأمن السيبراني للمسؤولين التنفيذيين. ومع ذلك، أظهر تحليل النضج أن كثيرًا من المناطق

تعاني قصور يستلزم معه بذلك المزيد من الجهود لوضع أدلة استرشادية تعمل على تعزيز هذه الأبعاد. وعند وضع كل ذلك في الاعتبار، يتبين لنا من درجات النضج التي أحرزتها كل مؤسسة على حدة، أن هناك نظرة متفائلة تجاه الأمن السيبراني، إذ تؤمن المؤسسات المعنية في مختلف أنحاء العالم بمدى أهميته الكبيرة في قطاع الرعاية الصحية. ولكن لا بد من بذل مزيد من الجهود لوضع إطار شامل للأمن السيبراني يتسم بالديناميكية في استجابته للهجمات السيبرانية التي تزداد طبيعتها تعقدًا يومًا بعد يوم.

القيود البحثية

ثمة قيود بحثية ينبغي مراعاتها عند تفسير نتائج الاستطلاع، أهمها هو صغر حجم العينة. فرغم أن النتائج نابعة من ستة مناطق جغرافية، لم يتجاوز حجم العينة ١٧ مؤسسة. وكانت هناك مناطق تتمتع بتمثيل أكبر من غيرها بعد انتهاء استطلاعات الرأي. ومن ثم، فإن إجراء الاستطلاع نفسه على عدد أكبر من المشاركين قد يفضي على نتائج مختلفة. وتجدر الإشارة إلى أن الاستطلاع أجري على عدد متنوع من المؤسسات، ويحتمل ألا تعبر النتائج تعبيرًا دقيقًا عن مشهد الأمن السيبراني لكل بيئة من بيئات الرعاية الصحية. كما أن الاستطلاع اعتمد على التقارير الذاتية التي يقدمها المشاركون، ولم يتسنى للفريق البحثي التحقيق من دقة هذه التقارير من جهة مستقلة.

الجزء الثاني: نتائج تقنية دلفي لتحقيق التوافق في الآراء

أجريت تقنية تحقيق التوافق في الآراء بشكل إلكتروني مع مجموعة من الخبراء يمثلون ١٦ دولة. وكان إجمالي المتطوعين ٣٤ متطوعًا، حيث شاركوا في جولة تحديد النطاق التي قاموا فيها بتحديد ٦٥ عنصرًا يرون أنه لا غنى عنها عند وضع إطار للأمن السيبراني. وتنوعت خبرات المشاركين، فمنهم من يعمل في قطاع الرعاية الصحية (٧ مشاركين) والحكومة (٧ مشاركين) والشركات (٦ مشاركين) والأوساط الأكاديمية (٥ مشاركين) والاستشارات المستقلة (٥ مشاركين) والتنمية/ المنظمات غير الحكومية (٤ مشاركين). وأجاب الخبراء على استبيانات قسمت على ثلاث جولات (من بينها جولة تحديد النطاق في البداية)، وقام المشرف على الاستبيانات بتقديم ملخص بالإجابات عقب كل جولة دون ذكر أسماء، موضحًا الأسباب الكامنة وراء اختيارات المشاركين. وسُئل المشاركون خلال جولة تحديد النطاق عن أهم عناصر إطار الأمن السيبراني، فخرجت الجولة بـ ٦٥ عنصرًا تم تصنيفها في ست فئات على يد الفريق البحثي (٤ باحثين).

وسئل ٣٣ مشاركًا في الجولة الأولى من الاستبيان عن مدى أهمية كل عنصر من العناصر الـ ٦٥ عند وضع إطار عالمي للأمن السيبراني بحيث تمنح إجاباتهم وفق مقياس يبدأ من ١ وينتهي عند ٩، وذلك من أجل تحقيق توافق في الآراء بشأن العناصر ذات الأولوية. وحظي ٥٩ عنصرًا بالإجماع على أهميتها عند وضع إطار عالمي للأمن السيبراني.

وبعد ذلك، أعدت مسودة لإطار عمل الأمن السيبراني بعد مراجعة العناصر الـ ٥٩ التي أجمع عليها المشاركون خلال الجولة الأولى، مع الإشارة في الوقت نفسه إلى تعليقات المشاركين. وأعقب ذلك إجراء نقاش بين أفراد الفريق البحثي.

وخلال الجولة الثانية، قام ٣٠ مشاركًا بتقييم المسودة، وتم التوصل إلى توافق في الآراء بشأن إطار الأمن السيبراني المقدم بعد الانتهاء من هذه الجولة.

القيود البحثية

ثمة قيود بحثية عند استشارة الخبراء، من بينها الانتشار الجغرافي لهؤلاء الخبراء. ورغم بذل ما بوسعنا من جهود لتمثيل عدد متنوع من الدول في هذا العمل البحثي، جاء معظم الخبراء من الدول ذات الدخل المرتفع، وجاءت نسبة مشاركة الدول ذات الدخل المتوسط ٢٣,٥٪. وفي الوقت نفسه، لم تمثل الدول ذات الدخل المنخفض في الاستبيانات رغم أن بعضًا من المشاركين سبق لهم العمل في بعضها مما جعلهم يكتسبون رؤى متخصصة بشأنها. ويبرز هذا القيد البحثي أحد صعوبات وضع إطار عالمي للأمن السيبراني، والمتمثل في ضعف خبرات الدول ذات الدخل المتوسط والمنخفض في هذا المجال. ولا بد من إجراء مزيد من البحوث في هذا المجال بحيث تستوعب مشاركة أكبر من الدول ذات الدخل المتوسط والمنخفض متى أمكن ذلك.

استخدام البحوث في وضع إطار العمل

في أعقاب تحليل حالة الأمن السيبراني على مستوى العالم، وتحقيق الإجماع بين الخبراء الذين شاركوا في تقنية دلفي، قمنا بإعداد نسخة أكثر شمولًا من الإطار العالمي للأمن السيبراني في مجال الرعاية الصحية – ألا وهو أساسيات الأمن السيبراني في مؤسسات الرعاية الصحية، والذي سنتناوله بالتفصيل في القسم الخامس.

القسم الخامس: وضع إطار عالمي للأمن السيبراني في مجال الرعاية الصحية

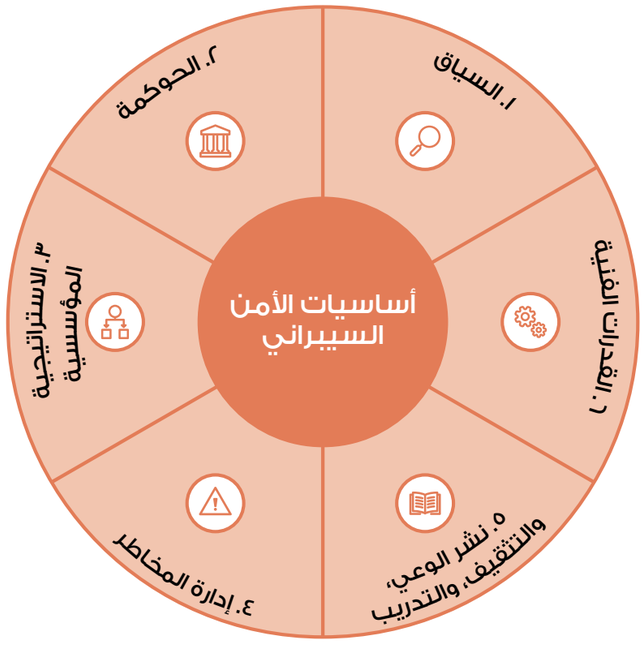
أطر الأمن السيبراني

تعد أطر الأمن السيبراني بمنزلة تتبناها المؤسسات بوجه عام لتعزيز المرونة السيبرانية وتحديد الخطوات اللازمة لحماية نفسها من الهجمات السيبرانية.[٥٩] أما في مجال الرعاية الصحية، فثمة اعتبارات تتعلق ببوجه خاص ببيانات المريض والصحة، كما أن له تكنولوجياته الخاصة المعنية بالرعاية الصحية. ولا يمكن رسم الخطط لمواجهة الهجمات السيبرانية وتحسين مستوى المرونة إلا بعد تحديد البيانات والأنظمة التي ينبغي حمايتها داخل أية مؤسسة من مؤسسات الرعاية الصحية.

إطار أساسيات الأمن السيبراني في مؤسسات الرعاية الصحية

أوضحنا في القسم الرابع أن إطار أساسيات الأمن السيبراني في مؤسسات الرعاية الصحية (انظر الشكل ١٦) وضع بعد مشاورات مع الخبراء والمتخصصين في مجالات الأمن السيبراني وتكنولوجيا المعلومات والمعلوماتية الصحية، ومع الفريق البحثي في جامعة إمبريال كوليدج لندن وشبكة الأنظمة الصحية الرائدة.

الشكل (١٦): إطار عمل أساسيات الأمن السيبراني في مؤسسات الرعاية الصحية



ويرتكز إطار الأساسيات على العناصر التي حددتها لجنة الخبراء باعتبارها أهم العناصر التي ينبغي إدراجها عند وضع إطار عالمي للأمن السيبراني في مجال الرعاية الصحية. ويحدد الإطار كذلك الأبعاد الستة الأساسية التي يجب مراعاتها عند توسيع نطاق الأمن السيبراني في أية مؤسسة من مؤسسات الرعاية الصحية، كما يقدم لغة مشتركة للقضايا الأساسية التي يلزم التعامل معها. ويمكن النظر إلى الإطار باعتباره دليلًا في أصغر صوره، أو إطار مرجعي طموح وفقًا لحجم موارد المؤسسة ونضجها على الصعيد السيبراني.

وسوف نتناول هنا كل بعد من أبعاد إطار الأساسيات بمزيد من التفصيل.

البعد الأول: السياق
يصف السياق الظروف الأوسع نطاقًا التي تعمل فيها المؤسسة وأنظمة تكنولوجيا المعلومات والأمن السيبراني. يأخذ السياق في الاعتبار الجوانب الاجتماعية والثقافية في تحديد أفضل الوسائل لتطبيق إجراءات الأمن السيبراني، وكذلك الاعتبارات المتعلقة بالموارد المالية المتاحة ومستوى النضج في تكنولوجيا المعلومات ومشهد الأمن السيبراني.
استعداد الموظفين لاعتماد عناصر الأمن السيبراني
مستوى نضج أنظمة تكنولوجيا المعلومات
العوامل والأعراف الثقافية التي تقوض الأمن أو تعززه
تكاليف التنفيذ (مثل الموارد المالية والبشرية)

السياق هو البعد الأول لإطار الأساسيات، ولا بد من وضع خطط للأمن السيبراني تجعله ملائمًا للسياق وتكفل له الاستدامة. ومن شأن العناصر التي تندرج تحت بعد "السياق" الإسهام في وضع خطط قابلة للاستدامة ويمكن توفير الموارد المالية اللازمة لها. خطط تعبر عن مستوى نضج المؤسسة وتلقى قبول أصحاب المصلحة في كافة قطاعات المؤسسة، بما في ذلك موظفو الخطوط الأمامية، وتكون في نظرهم قابلة للتنفيذ.

البعد الثاني: الحوكمة
يراد بالحوكمة السياسات والبروتوكولات الرامية إلى الحد من مخاطر تعرض أنظمة تكنولوجيا المعلومات للهجمات السيبرانية وذلك من خلال تطبيق ممارسات الأمن السيبراني. وتمارس الحوكمة غالبًا على مستويات متعددة – وهي المستويات الإقليمية والوطنية والمحلية – وتتطلب تضافر جهود العديد من المشاركين من داخل المؤسسة ومن خارجها
خطة الإبلاغ عن الحوادث
معايير المعلومات الصحية/ السريرية
الإبلاغ عن التهديدات لأصحاب المصلحة
عملية تقييم السلامة السريرية
المتطلبات التشريعية الوطنية والمحلية (مثل شهادة الأيزو ا.٧٠٠٢، واعتماد كريست، ولائحة المعهد الوطني للمعايير والتكنولوجيا، واللائحة العامة لحماية البيانات)
تطبيق سياسة مناسبة "للعمل من المنزل"، بالإضافة إلى سياسة "إحضار جهازك الخاص"
أدلة لأفضل الممارسات

الحوكمة الفنية
معايير الأجهزة الطبية
ضوابط النظام والمؤسسة/ معايير اختبارات الاختراق
بروتوكولات جدار الحماية

يسلط البعد الثاني الضوء على أهمية مشهد الحوكمة الذي تعمل فيه كل مؤسسة من مؤسسات الرعاية الصحية. فهناك متطلبات تشريعية وطنية ومحلية يجب مراعاتها عند توسيع نطاق الأمن السيبراني، إلى جانب الحوكمة الفنية التي تميز القطاع الصحي عن غيره من القطاعات (مثل معايير الأجهزة الطبية). ويجب أن تسعى المؤسسات أيضًا إلى تطوير نظام حوكمة خاصة بها على مستوى مجلس الإدارة يضمن الإبلاغ عن التهديدات والحوادث بشكل فعال.

البعد الثالث: الاستراتيجية المؤسسية
يراد بالاستراتيجية المؤسسية السياسات وعمليات التخطيط وتوزيع المسؤوليات الخاصة بتكنولوجيا المعلومات والأمن السيبراني على مستوى المؤسسة. ويجب أن تراعي الاستراتيجية المؤسسية الاعتبارات السياقية ومتطلبات الحوكمة ذات الصلة.
خطة استمرارية الأعمال (مثل خطة الاستجابة للحوادث السريرية، والنسخ الاحتياطي التلقائي للبيانات)
استراتيجية الأمن السيبراني المؤسسي (مثل تحديد المسؤوليات وتعيين الملكيات، وموازنة السلطات، ووضع إطار عمل لإدارة المخاطر)
وضع ميزانيات مناسبة لتعزيز الأمن السيبراني
وضع استراتيجية للاتصالات خاصة بالأمن السيبراني
مناقشة الأمن السيبراني في مجلس الإدارة بصفة منتظمة
إنشاء مجموعة توجيهية أمنية متعددة التخصصات داخل المؤسسة
وضع استراتيجية مشتريات (للأنظمة والتكنولوجيا) لدعم الأمن السيبراني

يحدد البعد الثالث للإطار مجالات الاستراتيجية المؤسسية الرئيسة والتي ينبغي وضعها للاسترشاد بها في عمليات تخطيط الأمن السيبراني وتحقيق استدامته. ولا غنى عن السعي لكسب التأييد وتوافق الآراء على المستوى الاستراتيجي داخل مؤسسات الرعاية الصحية. لذلك، يوصى بشدة بتناول قضية الأمن السيبراني على مستوى مجالس الإدارات أو الإدارات العليا، على أن يتم وضع خطة لاستمرارية الأعمال. ومن الضروري كذلك وضع آلية مناسبة للإشراف على الأمن السيبراني داخل المؤسسة لضمان استمرارية فعاليته ونجاحه.

البعد الرابع: إدارة المخاطر

يراد بإدارة المخاطر عملية تحديد التهديدات التي تتعرض لها أنظمة تكنولوجيا المعلومات والأمن السيبراني بالمؤسسة وتقييمها وتخفيف حدتها. ويتعلق القسم أدناه بتحديد المخاطر وتقييمها وتخفيف حدتها حيثما أمكن ذلك، على الرغم من أن العديد من العناصر تتشابك في كثير من المجالات.

تحديد المخاطر

مراقبة مشهد المخاطر خلال تطوره (اكتشاف التهديدات)

كشف عمليات التصيد والوقاية منها

تحديد الأصول وإدارتها (الأصل هو أي بيانات أو جهاز أو مكون آخر يدعم نقل المعلومات)

تعيين البيانات والشبكات

تحديد التبعيات في سلسلة التوريد بأكملها والشركاء الآخرين

تقييم المخاطر

تقييم المخاطر/ وتحديد مواطن الضعف (بما في ذلك الموردين الخارجيين، وإنترنت الأشياء، وتحديد الأجهزة القديمة/ التي لم تعالج أخطائها البرمجية)

الدروس المستفادة/ إجراء عمليات تقييم تحليلية للأسباب الجذرية وراء الحوادث السيبرانية

عمليات تدقيق النظام (إما بشكل أتوماتيكي أو على يد مدققين)

تخفيف حدة المخاطر

مراقبة شبكة الأنظمة وعمليات الدخول ووسائل التنبيه (مثل تحديث القائمة الشاملة التي تضم مواطن الضعف)

تطوير عمليات الطوارئ (إدراك ما لم يمكن توفير موارد مالية له وتحديد سبل التخفيف من حدة أحد المخاطر)

إدارة المخاطر الداخلية (بما في ذلك قابلية التشغيل البيني)

إدارة المخاطر الخارجية (بما في ذلك إمكانية التشغيل البيني)

وضع السيناريوهات/ المحاكاة (إجراء تدريبات محاكاة لممارسة للتدرب على التعامل مع الحوادث/ الهجمات السيبرانية الخطيرة)

الاستعانة بالغير لتدقيق الضوابط (إجراء تقييم خارجي لعمليات الأمن السيبراني)

تعد إدارة المخاطر هي البعد الأوسع نطاقًا في إطار السياسات، إذ أنه يتناول عمليات تحديد المخاطر وتقييمها وتخفيف حدتها في سياق الأمن السيبراني. ولا بد من بذل الجهود في مجال من هذه المجالات حتى يمكن مراقبة مناخ المخاطر، واكتشاف التهديدات المحتملة، وتقييم أهمية كل خطر على حدة، والوقوف على أي دروس مستفادة من الحوادث السابقة. ويجب على المؤسسات كذلك تطوير أنظمة والعمليات وصيانتها بحيث تقلل من المخاطر إلى أدنى حد. وجدير بالذكر أن إدارة المخاطر في سياق الأمن السيبراني داخل أنظمة الرعاية الصحية تشهد تطورًا مستمرًا، إذ أن عجلة الابتكارات المستمرة الرامية لإيجاد حلول وتكنولوجيات جديدة لتوفير خدمات الرعاية الصحية يسفر عن ظهور مزيد من المخاطر.

البعد الخامس: التوعية والتعليم والتدريب

يراد بهذا البعد الإجراءات التي يلزم اتخاذها لضمان تمتع جميع أصحاب المصلحة داخل المؤسسة (بما في ذلك الموظفين والمرضى) بالحد الأدنى من المعرفة أساسية بدور تكنولوجيا المعلومات والأمن السيبراني في تحقيق سلامة المرضى، وبالقدرة على إثارة أي مخاوف. ويجب كذلك تدريب المكلفين بمهام الأمن السيبراني تدريبًا مناسبًا.

إشراك الموظفين ونشر الوعي السيبراني

اتخاذ التدابير اللازمة لضمان اقتصار المسؤوليات السيبرانية على الأفراد المؤهلين والمدربين بشكل مناسب

تدريب الموظفين الفنيين، مع توفير الحد الأدنى من المعرفة بمجال الأمن السيبراني للموظفين

توفير المواد/ الموارد التي توضح اللوائح وأفضل الممارسات وأنظمة الإبلاغ السارية.

يعد التعليم والتدريب والوعي أحد العناصر الحاسمة الأخرى اللازمة لتوسيع نطاق الأمن السيبراني، إذ أن قوة منظومة الأمن السيبراني في مؤسسة ما تعكس مستوى مهارات الموظفين ودرجة تحفيزهم. ويحدد البعد الخامس مجالات التعليم والتدريب والوعي الرئيسة التي يجب أخذها في الاعتبار لإعداد الموظفين إعدادًا مناسبًا لإدارة تهديدات الأمن السيبراني ذات الصلة بمهامهم. ويمكن تطبيق هذا البعد بأية أساليب مرغوب فيها شريطة أن تتضمن معلومات واضحة يسهل الوصول إليها من قبل جميع الموظفين. فلا ينبغي أن يقتصر الأمن السيبراني على أقسام تكنولوجيا المعلومات وحدها، بل يجب أن يمتد ليشمل جميع الموظفين في جميع أنحاء المؤسسة.

البعد السادس: القدرات الفنية

يراد بالقدرات الفنية مجموعة المتطلبات الفنية اللازمة لحماية الأمن السيبراني. فينبغي تصميم التكنولوجيا في هذا السياق بحيث تدعم عمليات تقديم خدمات الرعاية وليس إعاقتها. واعتمادًا على الاعتبارات السياقية (مثل الاحتياجات المؤسسية والميزانية المتاحة وما إلى ذلك)، فيمكن الاستعانة بالمتطلبات الفنية التالية كدليل إرشادي إما لتوضيح الحد الأدنى من المتطلبات الأساسية أو ليكون قائمة طموحة ينبغي السعي إلى تحقيقها.

التحكم في الوصول (وفق مبادئ ترمي إلى تقليل مخاطر الوصول غير المصرح به)

كلمات المرور/ المصادقة – مصادقة الرسائل وإعداد تقاريرها وتوافقها استنادًا إلى النطاق/ إدارة الهويات/ المصادقة **متعددة العوامل**

تأمين الأجهزة الجوالة والأجهزة الطبية (بما في ذلك طرق التشخيص)

تكنولوجيات الكشف عن التهديدات والعمليات التي ترسل التنبيهات

–التصحيح المنتظم للأخطاء البرمجية وتحديثات البرامج

–تشفير البيانات

تجزئة الشبكة (تحسين الأمان والأداء عن طريق تقسيم شبكة الكمبيوتر إلى أجزاء أصغر للسيطرة بشكل أفضل على تدفقات المستخدمين للشبكة)

–مكافحة البرامج الضارة/ برامج مكافحة الفيروسات وجدران الحماية المناسبة

–إخفاء هوية أصحاب البيانات (عند توفير ملخصات البيانات للأعمال البحثية مثلًا)
قائمة مرجعية تحتوي على الحد الأدنى من الأجهزة والبرامج المطلوبة لإدارة معلومات المريض
تأمين البوابة (نوع من حلول الأمان الذي يمنع حركات المرور غير الآمنة، بما في ذلك الفيروسات/ والبرامج الضارة، من دخول الشبكة الداخلية للمؤسسة)
قدرات التخزين السحابي (ومعاييره) لضمان مستوى أفضل من الأمان

يرتبط البعد السادس لإطار أساسيات الأمن السيبراني في مؤسسات الرعاية الصحية بالقدرات الفنية للمؤسسات وعلاقتها بالأمن السيبراني. وتتنوع هذه القدرات تنوعًا كبيرًا داخل مؤسسات الرعاية الصحية. لذلك، من الأهمية بمكان ألا يتم النظر في عناصر هذا البعد بمعزل عن عناصر الأبعاد الأخرى، بل يتم استخدامها معًا لبناء ثقافة متينة للأمن السيبراني داخل المؤسسة. وتسلط عناصر البعد السادس الضوء على المجالات الرئيسة التي يجب مراعاتها عند رفع مستوى الأمن السيبراني عبر اكتساب القدرات الفنية المناسبة.

استخدام إطار أساسيات الأمن السيبراني في مؤسسات الرعاية الصحية

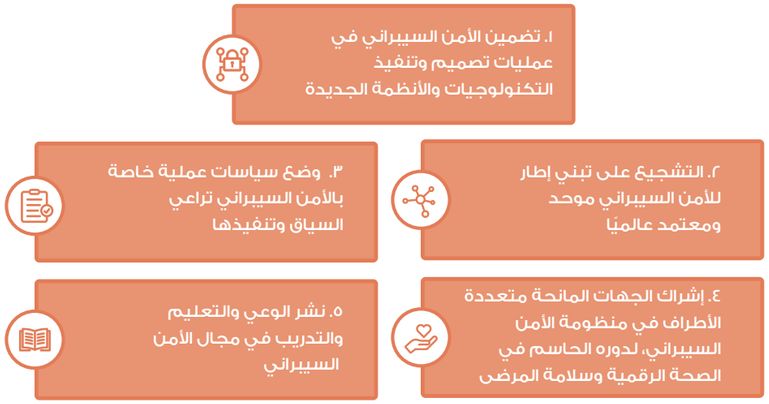
أغفلنا بعض العناصر الفنية عمدًا – مثل الذكاء الاصطناعي. فكما ذكرنا سابقًا، ليست غايتنا من وراء الإطار أن يكون مرجعًا إلزاميًا للمؤسسات، بل مجرد دليل إرشادي قابل للتطبيق في مؤسسات الرعاية الصحية في جميع أنحاء العالم. ويجب على المؤسسات ذات القدرات الفنية المتقدمة استخدام مبادئ الحوكمة وإدارة المخاطر والاسترشاد بها في تحديد القدرات الفنية التي يلزم إدراجها ضمن منظومة الأمن السيبراني لديها. وبذلك، فقد يكون إطار الأساسيات هذا مجرد «دليل إرشادي في أبسط صوره» في هذا السياق. أما بالنسبة للمؤسسات ذات القدرات الفنية الأقل تقدمًا، فعليها اعتبار البعد السادس حدها الأدنى من الدليل الإرشادي، دليل تطمح إلى تحقيقه وفقًا لسياقها واحتياجاتها.

القسم السادس: توصيات السياسة

يقدم هذا التقرير رؤية ثاقبة للوضع الحالي للأمن السيبراني داخل قطاع عريض من بيئات الرعاية الصحية في جميع أنحاء العالم. فيسلط الضوء على التحديات والفرص الحالية التي تواجهها أنظمة الرعاية الصحية عند تحقيق منظومة أمن سيبراني فعالة تعمل كعنصر أساسي في تحقيق سلامة المرضى.

وفيما يوفر إطار أساسيات الأمن السيبراني في مؤسسات الرعاية الصحية نقطة انطلاق لمقدمي خدمات الرعاية الصحية في العالم لتبني المرونة السيبرانية وتعزيزها في جميع البيئات، ما تزال هناك حاجة لاتخاذ مزيد من الخطوات حتى يكمن تعزيز جاهزية الأمن السيبراني في المستقبل. ويوضح الشكل (١٧) هذه الخطوات يليه توصياتنا المقترحة لإدخال تحسينات آمنة على استخدام البيانات والأنظمة الصحية بما يضمن سلامة المرضى.

الشكل (١٧): اللبنات الأساسية لتعزيز جاهزية الأمن السيبراني



١. تضمين الأمن السيبراني في تصميم التكنولوجيات والأنظمة الجديدة وتطبيقها

يلزم على الدول خلال سعيها إلى تعزيز النظم الصحية عبر الرقمنة أن تراعي الأمن السيبراني عند تصميم التكنولوجيات والأنظمة وعند تطبيقها. فعلى المستوى الوطني، يمكن اللجوء إلى إجراءات الحوكمة ووضع اللوائح المناسبة المعنية بالأمن السيبراني داخل قطاع الرعاية الصحية (مثل معايير الأجهزة الطبية) حتى نضمن اتباع أفضل الممارسات على المستوى المحلي. أما على المستوى المؤسسي، فينبغي تكليف مسؤولية الإشراف على الأمن السيبراني للأفراد الذين يتمتعون بحد أدنى من المعرفة بالتهديدات السيبرانية وحلولها.

٢. **السعي لوضع إطار موحد ومعتمد عالميًا للأمن السيبراني**

صمم إطار الجاهزية الوارد في هذا التقرير بحيث يمكن استخدامه في مختلف البيئات – أي في الدول ذات الدخل المرتفع والمنخفض والمتوسط على حد سواء – كما روعي أن تكون أولى خطواته هي وضع لغة مشتركة يفهمها الجميع. فعلى المستوى الوطني، ينبغي أن تنطوي أدلة السياسات الاسترشادية رفيعة المستوى على إطار عمل عالمي للأمن السيبراني. بينما على المستوى المؤسسي، فينبغي أن يوجه هذا الإطار عملية وضع خطط الأمن السيبراني واستدامتها. وتأتي هنا الخطوة الثاني، وهي اعتماد هذا الإطار على الصعيد العالمي، الأمر الذي يستلزم معه إبرام شراكات متينة لإجراء البحوث في مختلف المؤسسات بسياقاتها المختلفة ليتسنى لنا في نهاية المطاف الخروج بتوصيات أكثر دقة.

٣. **وضع سياسات عملية للأمن السيبراني تراعي السياق، ومن ثمّ تطبيقها**

لا بد من مراعاة المخاطر الماثلة وإمكانية التطبيق العملي عند وضع أي إجراءات أو سياسات للأمن السيبراني، بحيث تحد من هذه المخاطر بالشكل المناسب دون الإخلال بتوازن الموارد المطلوبة. ولا بد كذلك أن تحدد الحكومات سلم أولياتها من المهم فالأهم وتنفيذ التدخلات والأنظمة الفنية البسيطة التي لا تتطلب موارد ضخمة. ويتاح لمختلف المؤسسات حينئذ تقييم التكلفة الاقتصادية لتدخلات الأمن السيبراني بناءً على السياق والموارد المحلية المتاحة.

٤. **بناء جسور التواصل مع العديد من الجهات المانحة بشأن الأمن السيبراني لأهمية ذلك المحورية في الصحة الرقمية وسلامة المرضى**

لا يمكن تعزيز الجهود على المستوى العالمي دون توفر الموارد المالية والبشرية عند احتياجها، وهو الأمر الذي يزداد أهمية في الدول ذات الدخل المنخفض والمتوسط، إذ أن هذه الدول في حاجة إلى الدعم والمساعدة عند اختيار ممارسات الأمن السيبراني المستدامة وفي بناء خبراتها الفنية. فعلى المستوى الوطني، ينبغي أن تدخل وزارتا الصحة والمالية في نقاش لتحديد الأولويات اللازمة لتطوير القدرات الفنية داخل هيكل إدارتها وإدخال التكنولوجيا الصحية المناسبة في مؤسسات الرعاية الصحية. وينبغي عليهما كذلك تشجيع الجهات المانحة على مراعاة جوانب الأمن والمرونة وبناء القدرات الفنية في مخصصاتهم المالية. أما على المستوى المؤسسي، فينبغي التركيز على أهمية الأمن السيبراني وتضمينه عند وضع استراتيجية أوسع نطاقًا لتكنولوجيا المعلومات لأنها بمنزلة عامل مساعد للجهود الميدانية المنادية بمراعاة الأمن السيبراني في الاستثمارات الصحية العالمية.

٥. **نشر الوعي والتعليم والتدريب في مجال الأمن السيبراني**

لا يمكن إغفال ضرورة نشر الوعي بأهمية الأمن السيبراني داخل جميع مستويات الرعاية الصحية – بدءًا من المريض الذي ينبغي إشراكه في المسألة ومرورًا بالعاملين في الخطوط الأمامية الذين عليهم الإلمام بكيفية تضمين النظافة الإلكترونية في مهامهم الوظيفية وانتهاءً بواضعي الخطط والسياسات الصحية ممن ينبغي عليهم إدراك مدى أهمية الأمن السيبراني داخل مؤسساتهم ونظامهم الصحي بوجه عام. فعلى المستوى الوطني، ينبغي اكتساب الخبرة في وضع مناهج دراسية وطنية عن الأمن السيبراني في مجال الرعاية الصحية. أما على المستوى المؤسسي، فينبغي توفير الموارد التعليمية الخاصة بالأمن السيبراني لجميع الموظفين مع العمل على نشر ثقافة الوعي.

تتمتع الحلول الرقمية بالقدرة على إحداث ثورة في مجال الرعاية الصحية وتحسين صحة الأفراد في جميع أنحاء العالم، ولكن يلزم أولًا تحييد المخاطر المصاحبة للتهديدات السيبرانية. ونأمل أن يساعد إطار عمل أساسيات الأمن السيبراني في مؤسسات الرعاية الصحية وهذه التوصيات في توجيه صناع السياسات ومؤسسات الرعاية الصحية في تعزيز البنية التحتية للأمن السيبراني لديها، ومن ثمّ، حماية مرضاهم.

مسرد المصطلحات

سيبراني
يتعلق بأجهزة الكمبيوتر وتكنولوجيا المعلومات والواقع الافتراضي.

الهجوم السيبراني
محاولات خبيثة لإلحاق الضرر أو تعطيل أو الوصول غير المصرح به إلى أنظمة الكمبيوتر أو الشبكات أو الأجهزة عبر وسائل إلكترونية.

الحادث السيبراني
خرق لسياسة أمن النظام، من أجل التأثير على سلامته أو توفره، أو محاولة الوصول غير المصرح به إلى النظام.

النضج السيبراني:
المستوى الذي حققته المؤسسة في قدرتها على حماية أصول المعلومات الخاصة بها من التهديدات السيبرانية.

الجاهزية السيبرانية
حالة من الاستعداد أو القدرة على التصدي للهجمات السيبرانية.

التهديد السيبراني
فعل حالي أو محتمل يهدف إلى سرقة البيانات (الشخصية أو غيرها)، أو الإضرار بالبيانات، أو التسبب في أحد صور الضرر الرقمي.

الأمن السيبراني
ممارسة حماية البيانات والأنظمة والشبكات والبرامج من الهجمات السيبرانية.

البيانات
وحدات المعلومات الفردية التي تجمع معًا للرجوع إليها أو لتحليلها.

خرق البيانات
الإفشاء المتعمد أو غير المقصود عن معلومات آمنة أو خاصة/ سرية في بيئة غير موثوق بها

الصحة الإلكترونية
الرعاية الصحية المدعومة بعمليات إلكترونية بوجه عام.

الثغرة
قد تشير إلى البرامج أو البيانات التي تستغل ثغرة أمنية في النظام لإحداث عواقب غير مقصودة.

القرصنة
الوصول غير المصرح به إلى البيانات في نظام أو جهاز كمبيوتر.

القيادة (المؤسسية)
قد تشمل مجالس الإدارات أو اللجان التوجيهية أو أية قيادات أخرى داخل المؤسسة.

البرامج الضارة
يمكن استخدامها لسرقة البيانات أو مراقبة استخدام الجهاز أو التحكم في الأجهزة، ولكنها لا تصيب الأجهزة إلا بعد أن يقوم مستخدم مصرح له بتثبيتها على أجهزته عن طريق الخطأ أو غير ذلك.

الخدمات الصحية المتنقلة
حلول الرعاية الصحية التي تستخدم تكنولوجيا الاتصالات المتنقلة والأجهزة الشخصية الجوالة (مثل الهواتف الذكية والأجهزة اللوحية).

البرامج الضارة
يمكن استخدامها لسرقة البيانات أو مراقبة استخدام الجهاز أو التحكم في الأجهزة، ولكنها لا تصيب الأجهزة إلا بعد أن يقوم مستخدم مصرح له بتثبيتها على أجهزته عن طريق الخطأ أو غير ذلك.

برامج الفدية
برامج ضارة تجعل البيانات أو الأنظمة غير قابلة للاستخدام حتى يقوم الضحية بدفع الفدية.

آليات الإبلاغ
الأنظمة التي تتيح الإبلاغ عن الحوادث المشتبه في حدوثها أو الواقعة فعلًا وتثير المخاوف

الأمن حسب التصميم
تكنولوجيا المعلومات والبرمجيات التي تتضمن آليات للأمن في أبسط صورها.

المعلومات الحساسة
المعلومات أو البيانات التي يجب حمايتها من الوصول غير المصرح به والإفصاح غير المبرر، للحفاظ على الأمن المعلوماتي لفرد أو مؤسسة.

شكر وتقدير

أشرفت الدكتورة سائرة غافور (رئيس قسم الصحة الرقمية) على هذا التقرير وكتبته نيكي أوبراين (زميل سياسات في الصحة العالمية) والدكتورة إميليا جراس (زميل في الأمن السيبراني) والسيد جاي مارتن (محاضر سريري في المعهد الوطني للبحوث الصحية) ومعهد الابتكار في مجال الصحة العالمية بجامعة إمبريال كوليدج لندن. ونود أن نتقدم بالشكر للدكتور مايك دوركين، بمعهد الابتكار في مجال الصحة العالمية بجامعة إمبريال كوليدج لندن لقيادته شبكة الأنظمة الصحية الرائدة وإسهاماته في هذا التقرير.

ونود كذلك أن نشكر الأفراد والمؤسسات التالية أسماؤهم لمساهماتهم في هذا البحث (مرتبون ترتيبًا أبجديًا):

الأفراد

- سيف عابد
- علي عليدينا
- دينيس أندرسون
- هوتان أشرفيان
- ميكيل بيرموديز
- أنسيلمو بونسيرفيزي
- أدالبرتو كامبوس فرنانديز
- ديب شانا
- ستيفانو دالمياني
- راشيل دونسكومب
- أنورا فرناندو
- كلاريسا جاردنر
- دونيكا جيجولي
- نيكولاس جونزاليس
- كريس هانكين
- ريتشارد هاريسون
- وليام همفريز
- صامويل كيبت كيتر
- أنتوني كيتزلمان
- رامين كوزكاناني
- سابرينا تشينج يوين لوك
- كال ماركوكس
- أندريه ميجاتشيف
- أونيسموز موجيندي موانيكي
- آنا لويسا نيفيس
- ليانج تشي نين
- ين شين بان

- كولدو بينيرا إلورياجا
- ريتشارد بريس
- فارتان سركيسيان
- أرفيند سيفاراماكريشنان
- ألين أونجوريانو
- سام وامبوجو
- جون ويليامز
- بو وودز

المنظمات

- اتحاد الرعاية الصحية الإفريقي
- مستشفيات أبولو
- مؤسسة الباسك للابتكار والبحوث الصحية
- مستشفى شانجي العام
- وزارة الخارجية والكومنولث، المملكة المتحدة
- مؤسسة حمد الطبية
- هيئة مستشفيات هونج كونج
- صندوق هيئة الخدمات الصحية الوطنية للرعاية الصحية بجامعة إمبريال كوليدج
- المعهد الوطني للتميز في الخدمات الصحية والاجتماعية، كيبيك
- معهد الابتكار الصحي العالمي ، إمبريال كوليدج لندن
- لجنة تايوان المشتركة
- وزارة الصحة والخدمات الاجتماعية، كيبيك
- معهد رفاه لتعزيز الرعاية الصحية والسلامة
- المكتب الطبي الأوغندي البروتستانتي
- مجلس صحة مقاطعة ويتيماتا
- البنك الدولي

يتحمل المؤلفون مسؤولية أي أخطاء أو سهو.

نود أن نشكر فريق ويش على دعمهم وتوجيههم خلال إعداد هذا التقرير، وهم: نيكوليت ديفيز وجيانلوكا فونتانا، معهد الابتكار في مجال الصحة العالمية بجامعة إمبريال كوليدج لندن

المراجع

1. World Health Organization. *Draft Global Strategy on Digital Health 2020–2024*. Geneva: WHO; 2020. www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf?sfvrsn=f112ede5_42 [accessed 13 August 2020].

2. World Health Organization. *Draft Global Strategy on Digital Health 2020–2024*. Geneva: WHO; 2020. www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf?sfvrsn=f112ede5_42 [accessed 13 August 2020].

3. National Health Service. *The NHS Long Term Plan*. London: National Health Service; 2019. www.longtermplan.nhs.uk/wp-content/uploads/2019/08/nhs-long-term-plan-version-1.2.pdf [accessed 13 August 2020].

4. Ghafur S, et al. *Improving Cyber Security in the NHS*. London: Institute of Global Health Innovation, Imperial College London; 2019. www.imperial.ac.uk/media/imperial-college/institute-of-global-health-innovation/Cyber-report-2020.pdf [accessed 13 August 2020].

5. World Economic Forum. *Health Systems Leapfrogging in Emerging Economies: From concept to scale-up and system transformation*. Geneva: World Economic Forum; 2015. http://image-src.bcg.com/Images/Health_Systems_Leapfrogging_Emerging_Economies_2015_tcm38-79789.pdf [accessed 13 August 2020].

6. Makulilo AB. Privacy and data protection in Africa: A state of the art. *International Data Privacy Law*. 2012: 2(3), P163–78.

7. Mutale W, et al. Improving health information systems for decision making across five sub-Saharan African countries: Implementation strategies from the African Health Initiative. *BMC Health Services Research*. 2013; 13 (Suppl 2), S9.

8. Wambugu S, Villella C. *mHealth for Health Information Systems in Low- and Middle-Income Countries: Challenges and opportunities in data quality, privacy, and security*. Chapel Hill, USA: MEASURE Evaluation; 2014. www.measureevaluation.org/resources/publications/tr-16-140 [accessed 13 August 2020].

9. Bahia K, Suardi S. *Connected Society: The state of mobile internet connectivity 2019*. London: GSMA; 2019. www.gsma.com/mobilefordevelopment/resources/the-state-of-mobile-internet-connectivity-report-2019/ [accessed 13 August 2020].

10. Wambugu S, Villella C. *mHealth for Health Information Systems in Low- and Middle-Income Countries: Challenges and opportunities in data quality, privacy, and security*. Chapel Hill, USA: MEASURE Evaluation; 2014. www.measureevaluation.org/resources/publications/tr-16-140 [accessed 13 August 2020].

11. Talking Medicines. *What do all these 'health'-terms actually mean?* 6 March 2017. https://talkingmedicines.com/2017/03/digital-health-terms-ehealth-mhealth-telehealth-telemedicine/ [accessed 13 August 2020].

12. National Cyber Security Centre. *What is cyber security?* www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security [accessed 13 August 2020].

13. Organisation for Economic Co-operation and Development. *Cybersecurity Policy Making at a Turning Point: Analysing a new generation of national cybersecurity strategies for the internet economy*. Paris: OECD; 2012. www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf [accessed 13 August 2020].

14. Organisation for Economic Co-operation and Development. *Cybersecurity Policy Making at a Turning Point: Analysing a new generation of national cybersecurity strategies for the internet economy*. Paris: OECD; 2012. www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf [accessed 13 August 2020].

15. Hakmeh J, Shires J. *Is the GCC Cyber Resilient?* London: Chatham House; 2020. www.chathamhouse.org/publication/gcc-cyber-resilient [accessed 13 August 2020].

16. Ghafur S, et al. *Improving Cyber Security in the NHS*. London: Institute of Global Health Innovation, Imperial College London; 2019. www.imperial.ac.uk/media/imperial-college/institute-of-global-health-innovation/Cyber-report-2020.pdf [accessed 13 August 2020].

17. Świątkowska J. *Tackling Cybercrime to Unleash Developing Countries' Digital Potential*. Pathways for Prosperity Commission Background Paper Series; no. 33. Oxford: Pathways for Prosperity Commission; 2020. https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2020-01/tackling_cybercrime_to_unleash_developing_countries_digital_potential.pdf [accessed 13 August 2020].

18. Ghafur S, et al. *Improving Cyber Security in the NHS*. London: Institute of Global Health Innovation, Imperial College London; 2019. www.imperial.ac.uk/media/imperial-college/institute-of-global-health-innovation/Cyber-report-2020.pdf [accessed 13 August 2020].

19. Ghafur S, et al. *Improving Cyber Security in the NHS*. London: Institute of Global Health Innovation, Imperial College London; 2019. www.imperial.ac.uk/media/imperial-college/institute-of-global-health-innovation/Cyber-report-2020.pdf [accessed 13 August 2020].

20. Tham I, et al. *SingHealth cyber attack: How it unfolded*. The Straits Times, 20 July 2018. https://graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/sg-cyber-breach/index.html [accessed 13 August 2020].

21. Cunningham M, Towell N. *Surgeries delayed and patient security fears after cyber attack on Victorian hospitals*. The Age, 1 October 2019. www.theage.com.au/national/victoria/surgeries-delayed-and-patient-security-fears-after-cyber-attack-on-victorian-hospitals-20191001-p52wp1.html [accessed 13 August 2020].

22. Eddy N. *Alabama hospital system DCH pays to restore systems after ransomware attack*. Healthcare IT News; 7 October 2019. www.healthcareitnews.com/news/alabama-hospital-system-dch-pays-restore-systems-after-ransomware-attack [accessed 13 August 2020].

23. Miles R. *Life Healthcare announces cyberattack*. Intelligent CISO, 11 June 2020. www.intelligentciso.com/2020/06/11/life-healthcare-announces-cyberattack/ [accessed 13 August 2020].

24. World Health Organization. WHO reports fivefold increase in cyber-attacks, urges vigilance (press release), 23 April 2020. Geneva: World Health Organization; 2020. www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance [accessed 13 August 2020].

25. 2019 Public-Private Analytic Exchange Program. *A Lifeline: Patient Safety & Cybersecurity: Vulnerabilities of health information technology systems*. Washington DC: Department of Homeland Security, Office of Intelligence & Analysis, and the Office of the Director of National Intelligence. 2019. www.dhs.gov/sites/default/files/publications/ia/ia_vulnerabilities-healthcare-it-systems.pdf [accessed 13 August 2020].

26. Ghafur S, et al. A retrospective impact analysis of the WannaCry cyberattack on the NHS. *npj Digital Medicine*. 2019: 2(98).

27. Eddy M, Perlroth N. *Cyber attack suspected in German woman's death*. The New York Times, 18 September 2020. www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html [accessed 13 August 2020].

28. World Health Organization. *Global Spending on Health: A world in transition*. Geneva: WHO; 2019. www.who.int/health_financing/documents/health-expenditure-report-2019.pdf?ua=1 [accessed 13 August 2020].

29. Ghafur S, et al. *Improving Cyber Security in the NHS*. London: Institute of Global Health Innovation, Imperial College London; 2019. www.imperial.ac.uk/media/imperial-college/institute-of-global-health-innovation/Cyber-report-2020.pdf [accessed 13 August 2020].

30. Martin G, et al. Cybersecurity and healthcare: How safe are we? *BMJ*. 2017: 358, j3179.

31. National Institute of Standards and Technology (NIST). NIST Releases Version 1.1 of its Popular Cybersecurity Framework. NIST; 16 April 2018 (updated 16 January 2020). www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework [accessed 13 August 2020].

32. International Telecommunication Union (ITU). *Global Cybersecurity Index (GCI) 2018*. Geneva: ITU; 2018. www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf [accessed 13 August 2020].

33. Alshammari TS, Singh HP. Preparedness of Saudi Arabia to defend against cyber crimes: An assessment with reference to anti-cyber crime law and GCI index. *Archives of Business Research*, 2018: 6(12), P131–146.

34. Cyber Essentials. *About cyber essentials*. www.cyberessentialsonline.co.uk/about-cyber-essentials/ [accessed 13 August 2020].

35. NHS Digital. *Data Security and Protection Toolkit*. www.dsptoolkit.nhs.uk/ [accessed 13 August 2020].

36. IT Governance. *The DSP (Data Security and Protection) Toolkit*. www.itgovernance.co.uk/healthcare/dsp-toolkit [accessed 13 August 2020].

37. DeNisco Rayome A. *Does your organization need NIST, CSC, ISO, or FAIR frameworks? Here's how to start making sense of security frameworks*. TechRepublic. 7 March 2019. www.techrepublic.com/article/how-to-choose-the-right-cybersecurity-framework/ [accessed 13 August 2020].

38. DeNisco Rayome A. *Does your organization need NIST, CSC, ISO, or FAIR frameworks? Here's how to start making sense of security frameworks*. TechRepublic. 7 March 2019. www.techrepublic.com/article/how-to-choose-the-right-cybersecurity-framework/ [accessed 13 August 2020].

39. DeNisco Rayome A. Does your organization need NIST, CSC, ISO, or FAIR frameworks? Here's how to start making sense of security frameworks. *TechRepublic*. 7 March 2019. www.techrepublic.com/article/how-to-choose-the-right-cybersecurity-framework/ [accessed 13 August 2020].

40. DeNisco Rayome A. *Does your organization need NIST, CSC, ISO, or FAIR frameworks? Here's how to start making sense of security frameworks*. TechRepublic. 7 March 2019. www.techrepublic.com/article/how-to-choose-the-right-cybersecurity-framework/ [accessed 13 August 2020].

41. 2019 Public-Private Analytic Exchange Program. *A Lifeline: Patient Safety & Cybersecurity: Vulnerabilities of health information technology systems*. Washington DC: Department of Homeland Security, Office of Intelligence & Analysis, and the Office of the Director of National Intelligence. 2019. www.dhs.gov/sites/default/files/publications/ia/ia_vulnerabilities-healthcare-it-systems.pdf [accessed 13 August 2020].

42. Peter AS. Cyber resilience preparedness of Africa's top-12 emerging economies, *International Journal of Critical Infrastructure Protection*, 2017: 17, P49–59.

43. Global Partners Digital. *Multistakeholder Approaches to National Cybersecurity Strategy Development*. London: Global Partners Digital; 2018. www.gp-digital.org/wp-content/uploads/2018/06/Multistakeholder-Approaches-to-National-Cybersecurity-Strategy-Development.pdf [accessed 13 August 2020].

44. Global Partners Digital. *Multistakeholder Approaches to National Cybersecurity Strategy Development*. London: Global Partners Digital; 2018. www.gp-digital.org/wp-content/uploads/2018/06/Multistakeholder-Approaches-to-National-Cybersecurity-Strategy-Development.pdf [accessed 13 August 2020].

45. International Telecommunication Union (ITU). *Global Cybersecurity Index (GCI) 2018*. Geneva: ITU; 2018. www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf [accessed 13 August 2020].

46. Rwanda Ministry of Health. National Cyber Security Policy. March 2015. www.minict.gov.rw/fileadmin/Documents/National_Cyber_Security_Policy/Rwanda_Cyber_Security_Policy_01.pdf [accessed 13 August 2020].

47. Royal Australian College of General Practitioners (RACGP). *Computer and Information Security Standards: For general practices and other office-based practices* (Second Edition). East Melbourne: RACGP; 2013. www.racgp.org.au/FSDEDEV/media/documents/Running%20a%20practice/Practice%20standards/Computer-and-information-security.pdf [accessed 13 August 2020].

48. Martin G, et al. Cybersecurity and healthcare: How safe are we? *BMJ*. 2017; 358, j3179.

49. Hakmeh J, Shires J. *Is the GCC Cyber Resilient?* London: Chatham House; 2020. www.chathamhouse.org/publication/gcc-cyber-resilient [accessed 13 August 2020].

50. Catota FE, et al. Cybersecurity education in a developing nation: The Ecuadorian environment. *Journal of Cybersecurity*. 2019: 5(1), P2057–2085.

51. Gercke M. *Understanding Cybercrime: A guide for developing countries*. Geneva: International Telecommunication Union; 2011. www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_Guide_A5_12072011.pdf [accessed 13 August 2020].

52. Salamzada K, Shukur Z, Bakar MA. A framework for cybersecurity strategy for developing countries: Case study of Afghanistan. *Asia-Pacific Journal of Information Technology and Multimedia*, 2015: 4(1), P1–10.

53. Global Cyber Security Capacity Centre. *Cybersecurity Capacity Maturity Model for Nations (CMM)* Revised Edition. Oxford: Oxford Martin School, University of Oxford; 2016. https://cybilportal.org/wp-content/uploads/2020/05/CMM-revised-edition_09022017_1.pdf [accessed 13 August 2020].

54. eDelphi.org. *eDelphi 2020*. www.edelphi.org/ [accessed 13 August 2020].

55. Global Cyber Security Capacity Centre. *Cybersecurity Capacity Maturity Model for Nations (CMM)* Revised Edition. Oxford: Oxford Martin School, University of Oxford; 2016. https://cybilportal.org/wp-content/uploads/2020/05/CMM-revised-edition_09022017_1.pdf [accessed 13 August 2020].

56. Global Cyber Security Capacity Centre. *Cybersecurity Capacity Maturity Model for Nations (CMM)* Revised Edition. Oxford: Oxford Martin School, University of Oxford; 2016. https://cybilportal.org/wp-content/uploads/2020/05/CMM-revised-edition_09022017_1.pdf [accessed 13 August 2020].

57. Ghafur S, et al. *Improving Cyber Security in the NHS*. London: Institute of Global Health Innovation, Imperial College London; 2019. www.imperial.ac.uk/media/imperial-college/institute-of-global-health-innovation/Cyber-report-2020.pdf [accessed 13 August 2020].

58. Global Cyber Security Capacity Centre. *Cybersecurity Capacity Maturity Model for Nations (CMM)* Revised Edition. Oxford: Oxford Martin School, University of Oxford; 2016. https://cybilportal.org/wp-content/uploads/2020/05/CMM-revised-edition_09022017_1.pdf [accessed 13 August 2020].

59. Martin G, et al. Cybersecurity and healthcare: How safe are we? *BMJ*. 2017; 358: j3179.

شركاء أبحاث «ويش»

يعرب "ويش" عن امتنانه للدعم الذي قدمته وزارة الصحة العامة


مؤسسة قطر
Qatar Foundation
wise


مجلس قطر
للمباني الخضراء
QATAR GREEN
BUILDING COUNCIL
عضو في مؤسسة قطر
Member of Qatar Foundation


RIPHAH


سدرة للطب
Sidra Medicine


thebmj


UPMB
ACTS 1:7-8
"Health in Totality"


UCL


CHanGE


Waitemata
District Health Board
Best Care for Everyone

ISBN 978-1-9139910-3-6

www.wish.org.qa