# Examining the threat of cyber-attacks on health care during the COVID-19 pandemic

Saif F. Abed,[a] Sophie Allain-Ioos[a] and Nahoko Shindo[a]

## Introduction

Health systems globally have turned to digital transformation to enhance both the clinical quality and the cost-efficiency of their services. Beginning with the replacement of paper medical records and processes with digital alternatives, significant investments have been made in electronic health record (EHR) systems and in digital imaging and laboratory systems. The digital revolution has advanced to exploratrion of the use of artificial intelligence (AI) through clinical decision support tools.

While this transformation has many benefits, such as enhanced patient safety, it has also created digital dependence, which can be exploited by threatening actors, ranging from organized cyber-crime groups to violent extremists, in cyber-attacks. The aim of this report is to present the evolving threat of cyber-attacks, in particular ransomware, describe the associated risks of ransomware attacks on health-care delivery, and offer ways for assessing the risk of cyber-attacks on health systems as part of preparedness and resilience in anticipation of such deliberate events (DEs).

## The evolving threat of cyber-attacks

In the early 2010s, the majority of cyber-attacks on health care compromised the confidentiality of health-care data and, specifically, personally identifiable information (PII) and protected health information (PHI).[1] Prominent attacks targeted the largest health insurance companies in the United States of America (USA),

[1] Cawthra J et al. Securing data integrity against ransomware attacks: using the NIST Cybersecurity Framework and NIST Cybersecurity Practice Guides. Gaithersburg (FL): National Institute of Standards and Technology; 2020 (https://csrc.nist.gov/pubs/cswp/17/securing-data-integrity-against-ransomware-attacks/ipd).

# Menace liée aux cyberattaques dans le secteur de la santé pendant la pandémie de COVID-19

Saif F. Abed,[a] Sophie Allain-Ioos[a] et Nahoko Shindo[a]

## Introduction

Dans le monde entier, les systèmes de santé ont entrepris une transformation numérique qui a permis d'améliorer à la fois la qualité clinique et la rentabilité des services qu'ils proposent. Dans un premier temps, certains processus et dossiers médicaux sont passés du format papier au format numérique et des investissements substantiels ont été consacrés à la mise en place de systèmes de dossiers de santé électroniques (DSE), ainsi qu'à des solutions numériques pour les services d'imagerie et de laboratoire. Cette révolution numérique a progressé à tel point que l'on s'intéresse désormais au rôle que peut jouer l'intelligence artificielle en tant qu'outil d'aide à la prise de décision clinique.

Cette transformation a de nombreuses retombées positives, en particulier l'amélioration de la sécurité des patients, mais elle a également engendré des dépendances numériques qui peuvent être exploitées par des acteurs malveillants, qu'il s'agisse de groupes organisés de cybercriminels ou d'extrémistes violents, dans le cadre de cyberattaques. Ce rapport présente l'évolution de la menace liée aux cyberattaques, en particulier les attaques par rançongiciel («ransomware»), décrit les risques que présentent ces attaques pour la prestation des soins de santé, et propose des pistes pour évaluer les risques de cyberattaques contre les systèmes de santé dans le cadre des activités de préparation et de renforcement de la résilience en amont de ces actes délibérés.

## Évolution de la menace liée aux cyberattaques

Au début des années 2010, la plupart des cyberattaques dans le secteur de la santé visaient à compromettre la confidentialité des données de santé, et plus particulièrement des informations personnelles identifiables (PII, «personally identifiable information») et des informations de santé protégées (PHI, «protected health information»).[1] Les plus grandes compagnies d'assurance

[1] Cawthra J et al. Securing data integrity against ransomware attacks: using the NIST Cybersecurity Framework and NIST Cybersecurity Practice Guides. Gaithersburg (FL): National Institute of Standards and Technology; 2020 (https://csrc.nist.gov/pubs/cswp/17/securing-data-integrity-against-ransomware-attacks/ipd).

compromising approximately 78.8 million patient records.[2] Large-scale data breaches became a regular occurrence from 2014 onwards as cyber-crime groups found ways to monetize stolen PII and PHI, such as through insurance fraud.

In 2017, a dramatic cyber-attack caused a paradigm shift in health-care cyber-crime. On 12 May 2017, England's National Health Service (NHS) was hit by a national ransomware attack, called WannaCry.[3] This was not a targeted attack, but, due to the inherent vulnerability of the NHS at the time, approximately 683 NHS or affiliated organizations were affected by a global cyber crime. These included 27 health-care organizations that provide acute health-care services and 8% of primary-care practices. Five hospitals that provide acute care had to divert ambulances, as they were unable to provide safe, effective care because the WannaCry attack rendered critical digital applications unavailable.[3]

Since then, cyber-crime groups have recognized that clinical data and patient safety can be placed at risk by attacking digital infrastructure. They can therefore coerce health-care organizations into paying a financial ransom for reinstating access to their critical health-care information technology (IT) systems or retrieving stolen data. The trend accelerated during the coronavirus disease 2019 (COVID-19) pandemic, with law enforcement agencies, including the International Criminal Police Organization (INTERPOL), sharing warnings about the threat of cyber-attacks to the health sector in 2020.[4, 5] By 2021, the US Federal Bureau of Investigation had reported that over 148 health-care organizations in the USA alone had been affected by ransomware attacks.[6]

## What is ransomware?

Ransomware is a type of malicious software (malware) that infects digital systems and prevents end-users from accessing data and applications by encrypting key information.[7] For example, a ransomware attack could

maladie des États-Unis d'Amérique ont ainsi été la cible d'attaques majeures, au cours desquelles environ 78,8 millions de dossiers de patients ont été compromis.[2] Des violations massives de données sont devenues récurrentes à partir de 2014, les groupes de cybercriminels ayant trouvé des moyens de monétiser les PII et PHI volées, notamment en recourant à la fraude à l'assurance.

En 2017, une cyberattaque retentissante a marqué un tournant majeur de la cybercriminalité dans le secteur de la santé. Le 12 mai 2017, le National Health Service (NHS) anglais a été victime d'une attaque par rançongiciel à l'échelle nationale, appelée WannaCry.[3] Il ne s'agissait pas d'une attaque ciblée mais d'un acte cybercriminel d'envergure mondiale qui, en raison de vulnérabilités propres au NHS à l'époque, a touché environ 683 établissements membres du NHS ou affiliés à ce dernier, dont 27 établissements de santé dispensant des soins aigus et 8% des cabinets de soins primaires. Cinq hôpitaux dotés de services de soins aigus ont dû procéder à un détournement des ambulances vers d'autres centres. Les établissements touchés ont été dans l'incapacité de prodiguer des soins sûrs et efficaces compte tenu de l'impact majeur qu'a eu l'attaque WannaCry sur leurs services, certaines applications numériques essentielles étant devenues indisponibles.[3]

Dès lors, les groupes de cybercriminels ont compris qu'ils pouvaient mettre en péril les données cliniques et la sécurité des patients en s'attaquant à l'infrastructure numérique, et ainsi contraindre les établissements de santé à payer une rançon en échange du rétablissement de l'accès à leurs systèmes informatiques essentiels ou du recouvrement des données volées. Cette tendance s'est accélérée pendant la pandémie de COVID-19: en 2020, les organismes chargés de l'application des lois, dont l'Organisation internationale de police criminelle (INTERPOL), ont mis en garde contre la menace liée aux cyberattaques dans le secteur de la santé.[4, 5] En 2021, le Federal Bureau of Investigation (FBI) américain a indiqué que plus de 148 établissements de santé avaient fait l'objet d'attaques par rançongiciel rien qu'aux États-Unis d'Amérique.[6]

## Qu'est-ce qu'un rançongiciel?

Un rançongiciel («ransomware») est un type de logiciel malveillant qui infecte les systèmes numériques et chiffre certaines informations clés, empêchant ainsi les utilisateurs finaux d'accéder aux données et aux applications.[7] Par exemple, une

[2] New Hampshire joins multistate settlement over 2014 Anthem data breach. Concord (NH): New Hampshire Department of Justice, Office of the Attorney General; 2020 (https://www.doj.nh.gov/news/2020/20200930-anthem-data-breach.htm).

[3] Smart W. Lessons learned review of the WannaCry Ransomware Cyber Attack. London: Department of Health and Social Care; 2018 (https://www.england.nhs.uk/wp-content/uploads/2018/02/06_pb_08_02_18-lessons-learned-review-wannacry-ransomware-cyber-attack.pdf).

[4] Cybercriminals targeting critical health care institutions with ransomware. Lyon: INTERPOL; 2020 (https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-health care-institutions-with-ransomware).

[5] INTERPOL report shows alarming rate of cyberattacks during COVID-19. Lyon: INTERPOL; 2020 (https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19).

[6] Internet Crime Report 2021. Washington DC: Federal Bureau of Investigation, Internet Crime Complaint Center; 2021 ( https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf).

[7] Ransomware Protection and Response. Gaithersburg (MD): National Institute of Standards and Technology, NIST Computer Security Resource Center; 2022 (https://csrc.nist.gov/Projects/ransomware-protection-and-response).

[2] New Hampshire joins multistate settlement over 2014 Anthem data breach. Concord (NH): New Hampshire Department of Justice, Office of the Attorney General; 2020 (https://www.doj.nh.gov/news/2020/20200930-anthem-data-breach.htm).

[3] Smart W. Lessons learned review of the WannaCry Ransomware Cyber Attack. London: Department of Health and Social Care; 2018 (https://www.england.nhs.uk/wp-content/uploads/2018/02/06_pb_08_02_18-lessons-learned-review-wannacry-ransomware-cyber-attack.pdf).

[4] Cybercriminals targeting critical health care institutions with ransomware. Lyon: INTERPOL; 2020 (https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-health care-institutions-with-ransomware).

[5] INTERPOL report shows alarming rate of cyberattacks during COVID-19. Lyon: INTERPOL; 2020 (https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19).

[6] Internet Crime Report 2021. Washington DC: Federal Bureau of Investigation, Internet Crime Complaint Center; 2021 ( https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf).

[7] Ransomware Protection and Response. Gaithersburg (MD): National Institute of Standards and Technology, NIST Computer Security Resource Center; 2022 (https://csrc.nist.gov/Projects/ransomware-protection-and-response).

encrypt data in a hospital's network infrastructure, making critical clinical applications such as EHR platforms and medical imaging inaccessible to clinicians. There are various types of ransomware, the use of which depends on the objective and characteristics of the attack (e.g. crypto, locker). Currently, one of the most common forms is Ransomware as a Service (RaaS), which is a business model that enables threat actors to offer their cyber-crime services against a target of choice for a price.

In order for access to be returned, the perpetrators extort a fee (in other words, a ransom) to be paid. Payments are generally requested in cryptocurrencies, which are more difficult for criminal justice authorities to trace. In the USA, the average ransom paid is approximately US$ 131 000.[8]

Theoretically, once payment has been made, data and systems are decrypted and access to core applications is returned. In practice, the perpetrators are not always true to their word, and there have been examples in which system access was not returned or was returned with significant data loss. Furthermore, cyber-criminals are developing more threatening and profitable tactics, such as threatening to leak or sell sensitive data if ransoms are not paid (known as double extortion) and to use stolen PHI to extort others such as patients (known as triple extortion).[9]

## How does ransomware infect an organization?

The most common route for ransomware infection is through social engineering mediated by phishing. This typically involves a cyber-organized crime group sending e-mails that have been crafted to appear legitimate to unsuspecting end-users.[10] The e-mail contains either an attachment or a link that an end-user is persuaded to click on, which leads to malware being installed on their system. The malware that is immediately installed may be ransomware or it may be other malware which a cyber-crime group can use to hide and spread deeper into an organization's network before launching a ransomware attack. Although e-mail is the most common form of phishing, additional methods include SMS messaging ("smishing") and voice calls ("vishing").[11]

attaque par rançongiciel peut consister à chiffrer les données de toute l'infrastructure réseau d'un hôpital, de sorte que les cliniciens ne peuvent plus accéder aux applications cliniques essentielles telles que les plateformes de DSE ou les systèmes d'imagerie médicale. Il existe différents types de rançongiciels en fonction de l'objectif et des caractéristiques de l'attaque (crypto, locker, etc). L'une des formes d'attaques les plus courantes à l'heure actuelle repose sur le concept de «rançongiciel en tant que service» (RaaS, «Ransomware as a Service»), un modèle commercial dans le cadre duquel les acteurs malveillants proposent leurs services de cybercriminalité contre une cible au choix moyennant un certain prix.

Les auteurs extorquent une somme d'argent (en d'autres termes, une rançon) en échange du rétablissement de l'accès aux données. Les paiements sont généralement demandés en cryptomonnaies, qui sont plus difficiles à tracer pour les autorités judiciaires. Aux États-Unis d'Amérique, la rançon moyenne versée s'élève à environ 131 000 dollars (USD).[8]

En théorie, une fois le paiement effectué, les données et les systèmes sont censés être décodés et l'accès aux applications essentielles devrait être rétabli. Dans la pratique, les cybercriminels ne tiennent pas toujours leurs promesses et il est déjà arrivé que l'accès aux systèmes ne soit pas restauré et que des quantités importantes de données soient perdues. En outre, les cybercriminels ont fait évoluer leurs tactiques afin de les rendre encore plus menaçantes et rentables. Ainsi, ils peuvent menacer de divulguer ou de vendre des données sensibles si les rançons ne sont pas payées (double extorsion) ou d'utiliser les PHI volées pour extorquer de l'argent à d'autres personnes, par exemple aux patients (triple extorsion).[9]

## Comment un rançongiciel infecte-t-il une organisation?

L'infection par un rançongiciel résulte le plus souvent d'un acte d'ingénierie sociale reposant sur la technique de l'hameçonnage («phishing»). Il s'agit généralement d'un scénario où un groupe organisé de cybercriminels envoie des courriels conçus pour paraître légitimes à des utilisateurs finaux qui ne se doutent de rien.[10] Le courriel en question incite l'utilisateur à ouvrir un fichier joint ou à cliquer sur un lien, ce qui entraîne l'installation immédiate d'un logiciel malveillant («malware») sur son système. Ce logiciel malveillant peut être un rançongiciel, mais il peut aussi s'agir d'un autre type de logiciel utilisé par le groupe de cybercriminels pour rester dissimulé tout en s'infiltrant plus avant dans le réseau de l'organisation ciblée avant de lancer une attaque par rançongiciel. Bien que le courrier électronique soit le mode d'hameçonnage le plus courant, d'autres méthodes consistent à cibler les utilisateurs par le biais de messages SMS («smishing») ou d'appels vocaux («vishing»).[11]

[8] Ransomware Trends 2021. Washington DC: Department of Health and Human Services, HHS Cybersecurity Program, Office of Information Security; 2021 (https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf).

[9] The New Insider Threat: Are ransomware groups recruiting your employees? Black Fog, 7 March 2022 (https://www.blackfog.com/ransomware-groups-recruiting-your-employees/).

[10] Phishing. Gaithersburg (MD): National Institute of Standards and Technology, Small Business Cybersecurity Corner; 2022 (https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing).

[11] Drolet M. Smishing and vishing: How these cyber attacks work and how to prevent them. CSO Online, 8 August 2019 (https://www.csoonline.com/article/3411439/smishing-and-vishing-how-these-cyber-attacks-work-and-how-to-prevent-them.html).

[8] Ransomware Trends 2021. Washington DC: Department of Health and Human Services, HHS Cybersecurity Program, Office of Information Security; 2021 (https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf).

[9] The New Insider Threat: Are ransomware groups recruiting your employees? Black Fog, 7 March 2022 (https://www.blackfog.com/ransomware-groups-recruiting-your-employees/).

[10] Phishing. Gaithersburg (MD): National Institute of Standards and Technology, Small Business Cybersecurity Corner; 2022 (https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing).

[11] Drolet M. Smishing and vishing: How these cyber attacks work and how to prevent them. CSO Online. [Online] August 8, 2019 (https://www.csoonline.com/article/3411439/smishing-and-vishing-how-these-cyber-attacks-work-and-how-to-prevent-them.html).

Ransomware attacks have an element of social engineering that enables them to infect an organization, as their success relies on how convincing and persuasive the message is. For example, sending nursing staff an email that purports to be from their departmental manager with a file attachment that includes their upcoming rota details will appear more authentic than an email that states the recipient has won a prize and that they should click on a link to claim it. The former message will have a higher conversion rate in terms of malware execution.

Often, once a threat actor has access to an organization's network, it will look for software vulnerabilities and (human or software) misconfigurations that they can exploit to make their attacks more devastating and more difficult to resolve. Device or system infections may remain inactive in devices for long periods without their users being aware of them. Certain types of vulnerability allow attackers to potentially compromise networks without phishing e-mails. Remote desktop protocol (RDP) backdoor vulnerabilities are the most common examples that have been associated with ransomware attacks in health care.[8] Organizations face a problem, however, any time a device is Internet-facing and if it has vulnerabilities that allow it to be taken over remotely. This challege applies to any type of networked digital end-point. Research in 2019 identified diagnostic imaging servers containing approximately 400 million medical images that were readily accessible online.[12] RDP can also be exploited due to poor credential management by organizations or when threat actors obtain previously stolen credentials through the dark web.[13]

Another common source of compromise is "insider threat". This involves a person with legitimate access to an organization's systems who either intentionally or inadvertently uploads malware that could lead to a ransomware attack against a network.[9] The most common example is connecting an infected USB stick to a work computer, causing malware to be uploaded to the network. Personal online storage, email and messaging software are additional sources that can be used to compromise corporate networks by introducing malware.

## What happened during the COVID-19 pandemic?

During the COVID-19 pandemic, a sharp increase was noted in phishing attempts and ransomware attacks.[14] Many organizations became prime targets for ransom-

Pour infecter une organisation, les attaques par rançongiciel font appel à des techniques d'ingénierie sociale qui sont d'autant plus efficaces que le message est convaincant et persuasif. Par exemple, un courriel envoyé au personnel infirmier d'un établissement et provenant soi-disant du chef de service, avec un fichier joint détaillant leur planning à venir, semblera plus authentique qu'un courriel annonçant au destinataire qu'il a gagné un prix et qu'il doit cliquer sur un lien pour le réclamer. Parmi ces deux messages, c'est le premier qui convaincra le plus de destinataires et qui fera le plus de dégâts en permettant exécution du logiciel malveillant.

Souvent, une fois qu'ils ont réussi à accéder au réseau d'une organisation, les cybercriminels se mettent à la recherche de vulnérabilités logicielles ou d'erreurs de configuration (d'origine humaine ou logicielle) qu'ils pourraient exploiter pour rendre leurs attaques encore plus redoutables et difficiles à contrer. Des appareils ou des systèmes peuvent ainsi être touchés par des «infections» qui demeurent inactives pendant de longues périodes sans que les utilisateurs s'en rendent compte. Il existe aussi certains types de vulnérabilités qui permettent aux attaquants de compromettre des réseaux sans avoir besoin d'envoyer des courriels d'hameçonnage. Parmi ces vulnérabilités, l'accès par «porte dérobée» via le protocole RDP (Remote Desktop Protocol) est celle qui a le plus souvent donné lieu à des attaques par rançongiciel dans le secteur de la santé.[8] Cependant, tout appareil connecté à Internet qui présente des vulnérabilités susceptibles de le rendre contrôlable à distance représente un défi pour les organisations. Cela vaut pour tout type de terminal numérique en réseau. Des études menées en 2019 ont recensé des serveurs d'imagerie diagnostique contenant environ 400 millions d'images médicales facilement accessibles en ligne.[12] Les attaques exploitant le protocole RDP peuvent également résulter d'une mauvaise gestion des identifiants de connexion des utilisateurs par les organisations ou de situations où les acteurs de la menace se procurent des identifiants précédemment volés sur le «dark Web».[13]

Une dernière cause courante de compromission des données est ce qu'on appelle la menace interne. Dans ce scénario, une personne ayant un accès légitime aux systèmes d'une organisation télécharge, délibérément ou par inadvertance, un logiciel malveillant pouvant conduire à une attaque par rançongiciel contre un réseau.[9] L'exemple le plus courant est celui d'une clé USB infectée que l'utilisateur branche sur un ordinateur professionnel, ce qui entraîne le chargement d'un logiciel malveillant sur le réseau. L'accès à un espace personnel de stockage en ligne des données, le courrier électronique et les logiciels de messagerie sont autant de sources supplémentaires susceptibles d'être exploitées pour compromettre les réseaux d'une organisation par l'introduction de logiciels malveillants.

## Que s'est-il passé pendant la pandémie de COVID-19?

Au cours de la pandémie de COVID-19, on a assisté à une multiplication des tentatives d'hameçonnage et des attaques par rançongiciel.[14] Dans un contexte de connectivité accrue à

[12] Alder S. 400 million medical images are freely accessible online via unsecured PACS. Lansing (MI): HIPAA Journal, 18 September 2019 (https://www.hipaajournal.com/400-million-medical-images-are-freely-accessible-online-via-unsecured-pacs/).

[13] Whitney L. How one attack campaign steals and sells RDP credentials. Nashville (TN): TechRepublic. TechnologyAdvice, 17 August 2020 (https://www.techrepublic.com/article/how-one-attack-campaign-steals-and-sells-rdp-credentials/).

[14] Gravé-Lazi L. COVID-19 pandemic sparks 72% increase in ransomware attacks . The Jerusalem Post, 3 August 2020 (https://www.jpost.com/cybertech/covid-19-pandemic-sparks-72-percent-increase-in-ransomware-attacks-635935).

[12] Alder S. 400 million medical images are freely accessible online via unsecured PACS. Lansing (MI): HIPAA Journal, 18 September 2019 (https://www.hipaajournal.com/400-million-medical-images-are-freely-accessible-online-via-unsecured-pacs/).

[13] Whitney L. How one attack campaign steals and sells RDP credentials. Nashville (TN): TechRepublic. TechnologyAdvice, 17 August 2020 (https://www.techrepublic.com/article/how-one-attack-campaign-steals-and-sells-rdp-credentials/).

[14] Gravé-Lazi L. COVID-19 pandemic sparks 72% increase in ransomware attacks . The Jerusalem Post, 3 August 2020 (https://www.jpost.com/cybertech/covid-19-pandemic-sparks-72-percent-increase-in-ransomware-attacks-635935).

ware attacks due to increased connectivity to the Internet, rising demand on health-care systems and supply chains and severe resource constraints. Cyber-crime groups used the clear logic that the greater the risks to patient safety and for service disruptions they could create for an organization, the more likely it was that they would receive a ransomware payment.

Attacks were seen as early as March 2020 on acute health-care facilities that were both COVID-19 treatment centres and testing laboratories. This was the case at Brno University Hospital in Czechia, where a ransomware attack caused its leadership team to shut down its network, transfer patients to neighbouring institutions, postpone planned patient procedures and ask staff to resort to inefficient paper-based processes.[15] The attack occurred when the nation had just entered a state of emergency due to the pandemic.

On 14 May 2021, one of the largest, most devastating attacks on health care occurred when the Conti Ransomware Gang compromised the Irish Health Service Executive (HSE). This was achieved when an unsuspecting end-user viewed a phishing email containing a spreadsheet attachment. When it was opened, malware was downloaded that provided access to the network, allowing the malware to establish a foothold and spread throughout multiple parts of the HSE over 2 months. Once the Conti ransomware was triggered, it had a national impact, with approximately 80% of data in the system being encrypted, the national diagnostic imaging platform becoming inaccessible and radiotherapy services being paused in 5 major centres.[16] Because of the loss of access to patient details, appointments and medical records, over 50% of acute hospitals postponed outpatient appointments and elective clinical investigations and interventions.[16] In many organizations, clinical staff had to resort to paper-based processes in order to maintain baseline clinical services.

Recent surveys have demonstrated that not only have attacks been more targeted to the health care sector but they have increased in both scale and frequency. In 2021, in a large-scale survey of health care in the USA, approximately 43% of respondents reported having been subjected to 2 ransomware attacks during the preceding 2 years.[17] Interestingly, the proportion of respondents who lacked confidence in their organization's ability to manage the risks associated with ransomware attacks increased during 2020–2021 to 61% from 55% pre-pandemic.[17]

Internet, de demande croissante pesant sur les systèmes de santé et les chaînes d'approvisionnement et de ressources très limitées, de nombreuses organisations sont devenues des cibles privilégiées pour les attaques par rançongiciel. Le raisonnement des groupes de cybercriminels était simple: plus ils parviendraient à créer des risques pour la sécurité des patients et la continuité des services dans un établissement, plus ils avaient de chances de recevoir une rançon après une attaque par rançongiciel.

Dès mars 2020, des attaques ont été perpétrées contre des établissements de soins aigus qui abritaient à la fois des services de traitement de la COVID-19 et des laboratoires d'analyse. Ce fut le cas de l'hôpital universitaire de Brno en République tchèque. À la suite d'une attaque par rançongiciel, l'équipe de direction de cet hôpital a dû décider de mettre son système informatique à l'arrêt, de transférer des patients vers des établissements voisins et de reporter certaines interventions médicales planifiées, et le personnel a dû recourir à des processus sur support papier révélés inefficaces.[15] Cet incident s'est produit alors que l'état d'urgence venait d'être déclaré dans le pays en raison de la pandémie.

Le 14 mai 2021, l'une des attaques les plus massives et les plus dévastatrices qu'ait connues le secteur de la santé a été lancée par le Conti Ransomware Gang à l'encontre du système de santé irlandais, le Health Service Executive (HSE). Le point de départ de cette attaque a été l'ouverture, par un utilisateur peu méfiant, d'un courriel d'hameçonnage contenant une feuille de calcul en pièce jointe. Cela a mené à l'installation d'un logiciel malveillant fournissant un accès au réseau, ce qui a permis au logiciel de s'implanter et de s'infiltrer dans de nombreuses structures du HSE sur une période de 2 mois. Une fois que le rançongiciel Conti a été activé, son impact s'est manifesté à l'échelle nationale: environ 80% des données du système ont été chiffrées, la plateforme nationale d'imagerie diagnostique est devenue inaccessible et les services de radiothérapie ont été suspendus dans 5 grands centres.[16] La perte d'accès aux données des patients, aux informations sur les rendez-vous et aux dossiers médicaux a contraint plus de 50% des hôpitaux de soins aigus à reporter les rendez-vous ambulatoires et les interventions/examens cliniques non urgents.[16] Dans de nombreux établissements, le personnel clinique a dû recourir à des processus sur support papier afin de maintenir les services cliniques de base.

Des enquêtes récentes montrent non seulement que le secteur de la santé est devenu une cible privilégiée, mais aussi que les attaques ont gagné en ampleur et en fréquence. Dans une enquête à grande échelle menée en 2021 auprès des services de santé aux États-Unis d'Amérique, environ 43% des personnes interrogées ont déclaré avoir subi 2 attaques par rançongiciel au cours des 2 années précédentes.[17] Il est intéressant de noter que la proportion de personnes interrogées qui disent ne pas avoir confiance dans la capacité de leur organisation à gérer les risques associés aux attaques par rançongiciel a augmenté: elle était de 61% en 2020-2021, contre 55% avant la pandémie.[17]

[15] Brno University Hospital ransomware attack (2020). The NATO Cooperative Cyber Defense Centre of Excellence, International Cyber Law; 2021 (https://cyberlaw.ccdcoe.org/wiki/Brno_University_Hospital_ransomware_attack_(2020)).

[16] Conti cyber attack on the HSE. Independent Post Incident Review. Dublin: Health Service Executive, 2021 (https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf).

[17] The impact of ransomware on health care during COVID-19 and beyond. Traverse City (MI): Ponemon Institute LLC, 2021 (https://www.healthcareview.media/uploads/resources/resources/210202211333AM_Resource_TheImpactOfRansomwareOnHealthcareDuringCovid19AndBeyond.pdf).

[15] Brno University Hospital ransomware attack (2020). The NATO Cooperative Cyber Defense Centre of Excellence, International Cyber Law; 2021 (https://cyberlaw.ccdcoe.org/wiki/Brno_University_Hospital_ransomware_attack_(2020)).

[16] Conti cyber attack on the HSE. Independent Post Incident Review. Dublin: Health Service Executive, 2021 (https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf).

[17] The impact of ransomware on health care during COVID-19 and beyond. Traverse City (MI): Ponemon Institute LLC, 2021 (https://www.healthcareview.media/uploads/resources/resources/210202211333AM_Resource_TheImpactOfRansomwareOnHealthcareDuringCovid19AndBeyond.pdf).

A global survey of 328 IT leadership stakeholders in the health sector in 2021 revealed similar trends. Over a third of respondents reported at least 1 ransomware attack in the preceding year, and one third of those affected paid a ransom.[18] Even when ransom payments were made, 31% of respondents reported that they had not regained access to their encrypted data. There was no guarantee that the attackers would restore data or that any decryption keys would return data to the pre-attack state. Of the respondents that had not been impacted by ransomware, 41% reported that they expected to be victims of ransomware attacks in the future in view of the increasing prevalance of attacks in their sectors.[18]

Although the main focus of ransomware attacks has been health-care delivery organizations, during the COVID-19 pandemic, greater attention was paid to the broader biomedical supply chain. For example, security researchers identified readily exploitable RDP vulnerabilities in at least 17 biomedical companies involved in manufacturing COVID-19 vaccines and developing therapeutics.[19] One of the most prolific ransomware strains in health care, known as Ryuk, has been detected in attacks on life science institutes.[20] Further attacks have been reported against clinical trial software vendors, laboratories and pharmaceutical companies.[21]

## Why is health care a target?

The emergence of health care as a preferred target for cyber-attackers is relatively recent. As with all criminal acts, 3 factors should be considered – means, motive and opportunity.

In general, it has become easier (the means) for threat actors to conduct ransomware attacks; therefore, the pool of threat actors has broadened to include an increasing number of organized crime entities and even terrorist groups. High technical skill is no longer a prerequisite because of the development of new economic models by cyber-crime groups. Ransomware as a Service (RaaS) gangs now develop sophisticated ransomware, and their skills, tools or both can be licensed by less technically adept threat actors to target organiza-

Une enquête mondiale menée en 2021 auprès de 328 responsables informatiques dans le secteur de la santé a mis en évidence des tendances similaires. Plus d'un tiers des personnes interrogées ont fait état d'au moins une attaque par rançongiciel au cours de l'année précédente et un tiers des personnes touchées ont payé une rançon.[18] Même après le versement d'une rançon, 31% des personnes interrogées ont indiqué qu'elles n'avaient pas retrouvé l'accès à leurs données chiffrées. Rien ne permet de garantir que les cybercriminels restitueront les données ou fourniront des clés de déchiffrement permettant effectivement de restaurer les données identiques à leur état antérieur à l'attaque. Parmi les personnes interrogées qui n'avaient pas été victimes de rançongiciels, 41% ont déclaré qu'elles s'attendaient à subir des attaques par rançongiciel à l'avenir, compte tenu de la fréquence croissante de ces attaques dans leur secteur.[18]

Bien que les auteurs d'attaques par rançongiciel prennent principalement pour cible les organismes de prestation des soins, ils ont aussi commencé, pendant la pandémie de COVID-19, à s'intéresser plus globalement à la chaîne d'approvisionnement biomédicale. Par exemple, des chercheurs en sécurité ont découvert qu'au moins 17 entreprises biomédicales impliquées dans la fabrication des vaccins contre la COVID-19 et dans la mise au point de produits thérapeutiques présentaient des vulnérabilités facilement exploitables du protocole RDP.[19] L'une des souches virales de rançongiciel les plus répandues dans le secteur de la santé, connue sous le nom de Ryuk, a été détectée dans des attaques menées contre des instituts de recherche en sciences de la vie.[20] D'autres attaques ont été signalées contre des fournisseurs de logiciels d'essais cliniques, des laboratoires et des sociétés pharmaceutiques.[21]

## Pourquoi le secteur de la santé est-il pris pour cible?

Le fait que les services de santé soient devenus une cible privilégiée des cyberattaquants est un phénomène relativement récent. Comme pour tout acte criminel, il convient de prendre en compte 3 facteurs essentiels: les moyens, les motifs et les opportunités.

S'agissant des moyens: d'une manière générale, il est devenu plus facile de mener des attaques par rançongiciel, ce qui signifie que le cercle des cybercriminels potentiels s'est élargi pour inclure un nombre croissant d'entités criminelles organisées et même de groupes terroristes. Compte tenu des nouveaux modèles économiques élaborés par les groupes de cybercriminels, il n'est plus nécessaire de posséder des compétences techniques de haut niveau pour participer à ces attaques. Désormais, des gangs spécialisés dans le «rançongiciel en tant que service» (RaaS) développent des rançongiciels sophistiqués et

[18] Mahendru P. The state of ransomware in healthcare 2021. Oxford: Sophos Ltd, 2021 (https://news.sophos.com/en-us/2021/05/17/the-state-of-ransomware-in-healthcare-2021/).

[19] Davis J. Report finds serious flaws in COVID-19 vaccine developers' systems. HealthITSecurity.net. Xtelligent Media, 17 July 2020 (https://healthitsecurity.com/news/report-finds-serious-flaws-in-covid-19-vaccine-developers-systems).

[20] Osborne C. Ryuk ransomware finds foothold in bio research institute through student who wouldn't pay for software. ZDNet., 6 May 2021 (https://www.zdnet.com/article/ryuk-ransomware-finds-foothold-in-bio-research-institute-through-a-student-who-wouldnt-pay-for-software/).

[21] Alder S. Clinical trial software provider hit with ransomware attack. Lansing (MI): HIPAA Journal, 5 October 2020 (https://www.hipaajournal.com/clinical-trial-software-provider-hit-with-ransomware-attack/).

[18] Mahendru P. The state of ransomware in healthcare 2021. Oxford: Sophos Ltd, 2021 (https://news.sophos.com/en-us/2021/05/17/the-state-of-ransomware-in-healthcare-2021/).

[19] Davis J. Report finds serious flaws in COVID-19 vaccine developers' systems. HealthITSecurity.net. Xtelligent Media, 17 July 2020 (https://healthitsecurity.com/news/report-finds-serious-flaws-in-covid-19-vaccine-developers-systems).

[20] Osborne C. Ryuk ransomware finds foothold in bio research institute through student who wouldn't pay for software. ZDNet., 6 May 2021 (https://www.zdnet.com/article/ryuk-ransomware-finds-foothold-in-bio-research-institute-through-a-student-who-wouldnt-pay-for-software/).

[21] Alder S. Clinical trial software provider hit with ransomware attack. Lansing (MI): HIPAA Journal, 5 October 2020 (https://www.hipaajournal.com/clinical-trial-software-provider-hit-with-ransomware-attack/)..

tions.[22] From a financial perspective, threat actors split the proceeds of any successful attack, ranging from the ransom payment to money made from selling exfiltrated PII/PHI. Threat actors that are not motivated solely financially, such as terrorist groups, can achieve their goals of spreading fear and attaining publicity without requiring the sophisticated technical skills necessary for executing a disruptive attack.

The motives for ransomware attacks are, at least superficially, financial. Recent data have shown that up to a third of affected health-care organizations have been willing to make ransom payments.[8] When combined with other sources of profit, such as trading stolen PHI/PII or security data (for example administrator login credentials), this has created an attractive return on investment for cyber-crime groups. The rise of health-care cyber-insurance specifically covering ransomware attacks and payments has, at least anecdotally, been seen as a further motivator for threat actors, as they may consider that insured health-care providers will be more likely to both pay and at higher amounts.[23] The increasing recognition that health-care organizations are part of critical national infrastructure has enhanced their attractiveness for cyber-crime groups, as they consider that they can seek higher ransoms if they disrupt essential services.

Furthermore, while national and regional cyber incident response teams have developed the capability to detect and prevent some ransomware attacks, most attacks are not reported to the criminal justice system. Even fewer are resolved with clearly identified responsible individuals or organizations. Therefore, ransomware is a crime that benefits from a high degree of impunity, and it is considered financially efficient, as the risks are relatively low while the rewards are lucrative.

Opportunities to attack health-care organizations on all continents, irrespective of their digital maturity, has been accelerated by the COVID-19 pandemic. Rapid digital transformation of health-care services to cope with the rising pressure on clinical services created even greater incentives for cyber-criminals to target hospitals and associated critical infrastructure. For example, in Europe and North America there has been an aggressive drive to replace paper-based workflows with digital alternatives. Regulations and government investments have accelerated this trend, hospitals being

peuvent céder sous licence leurs compétences ou leurs outils, voire les deux, à des acteurs de la menace techniquement moins compétents qui souhaitent cibler une organisation.[22] D'un point de vue financier, les acteurs partagent ensuite les bénéfices de toute attaque réussie, qu'il s'agisse du paiement d'une rançon ou de l'argent tiré de la vente de PII/PHI extrafiltrées. Les acteurs dont la motivation n'est pas uniquement financière, tels que les groupes terroristes, peuvent atteindre leurs objectifs, qui sont de semer la peur et se faire connaître, sans avoir les compétences techniques sophistiquées nécessaires à l'exécution d'une attaque fortement perturbatrice.

S'agissant des motifs: les attaques par rançongiciel sont motivées, du moins superficiellement, par des considérations financières. Des données récentes ont montré que jusqu'à un tiers des établissements de santé touchés avaient accepté de payer une rançon.8 Cette source de profit, combinée à d'autres, comme le commerce de PHI/PII volées ou de données de sécurité (par exemple, identifiants de connexion des administrateurs), représente un retour sur investissement très intéressant pour les groupes de cybercriminels. L'essor des cyberassurances dans le secteur de la santé, qui couvrent spécifiquement les attaques par rançongiciel et les paiements associés, peut être considéré, du moins de manière anecdotique, comme un facteur de motivation supplémentaire pour les cybercriminels, ces derniers pouvant en effet supposer que les prestataires de soins ayant contracté une assurance sont plus susceptibles de payer une rançon et que le montant versé pourrait être plus élevé.[23] Le fait que les établissements de santé soient reconnus comme des infrastructures nationales essentielles, fait d'eux une cible d'autant plus attrayante pour les groupes de cybercriminels, qui s'attendent à pouvoir toucher des rançons plus élevées lorsqu'ils perturbent des services essentiels.

En outre, bien que les équipes chargées de la gestion des incidents de cybersécurité au niveau national et régional aient acquis des capacités leur permettant de détecter et de prévenir certaines attaques par rançongiciel, la majorité des attaques ne sont pas signalées au système de justice pénale. Il est encore plus rare qu'elles soient résolues et que les personnes ou les organisations responsables soient clairement identifiées. En ce sens, l'attaque par rançongiciel est un crime qui bénéficie d'un haut degré d'impunité et qui est donc considéré comme rentable sur le plan financier, puisque les risques sont relativement faibles alors que les gains sont considérables.

S'agissant des opportunités: sur tous les continents, la pandémie de COVID-19 a favorisé les possibilités d'attaquer les établissements de santé, quel que soit leur niveau de maturité numérique. La transformation numérique rapide des services de santé, destinée à répondre aux pressions croissantes exercées sur les services cliniques, a incité encore davantage les cybercriminels à cibler les hôpitaux et les infrastructures critiques associées. Par exemple, en Amérique du Nord et en Europe, des efforts énergiques ont été déployés pour remplacer les flux de travail accomplis sur support papier par des solutions numériques. Les réglementations et les investissements consentis par

[22] Kostka C. Ransomware-as-a-service: an example for Big Tech? Ransomware.org; 26 January 2022 (https://ransomware.org/blog/ransomware-as-a-service-an-example-for-big-tech/).

[23] Shavell R. Why "ransomware insurance" causes health care industry to overlook deeper, underlying security issues. Rezonen Pte Ltd: CPO Magazine, 2 September 2021 (https://www.cpomagazine.com/cyber-security/why-ransomware-insurance-causes-health care-industry-to-overlook-deeper-underlying-security-issues/).

[22] Kostka C. Ransomware-as-a-service: an example for Big Tech? Ransomware.org; 26 January 2022 (https://ransomware.org/blog/ransomware-as-a-service-an-example-for-big-tech/).

[23] Shavell R. Why "ransomware insurance" causes health care industry to overlook deeper, underlying security issues. Rezonen Pte Ltd: CPO Magazine, 2 September 2021 (https://www.cpomagazine.com/cyber-security/why-ransomware-insurance-causes-health care-industry-to-overlook-deeper-underlying-security-issues/).

incentivized to increase their digital maturity according to industry standards, such as the HIMSS Electronic Medical Record Adoption Model rating scale.[24]

As paper records have been replaced, health-care organizations have had to rely on the sprawling, complex supply chains of software and hardware vendors to manage their digital ecosystems. They must also contend with further complexities, such as applications in the cloud, remote working and adoption of AI for clinical decision support. This increase in digital maturity has not been matched by equal investment or enhancement in cybersecurity maturity. The chasm between digital and cybersecurity maturity has left health-care organizations highly dependent on digital workflows but also vulnerable. Health-care organizations are often unaware of the breadth of technology that exists in their enterprise, how vulnerable it is and what the consequences for patient safety would be if it were compromised. When coupled with a lack of security professionals and leadership in the sector, these circumstances create numerous opportunities for targeting and compromising health-care organizations.

## What is the impact of ransomware on health outcomes?

The impact of ransomware attacks is often cited in fiscal terms. For example, in the USA, the average cost of a ransom payment is in excess of US$ 100 000, and total recovery costs are over US$ 1 million.[8] The HSE ransomware attack was estimated to have cost the Irish taxpayer over € 100 million.[25] Financial measures are not, however, indicative of the clinical risks associated with ransomware attacks or the public health impact.

In order to better understand these elements, we reviewed the 2 largest attacks seen to date. The WannaCry attack on the NHS caused 5 acute health-care organizations to divert ambulances for 3 days and a significant number of organizations to lack diagnostic imaging. In addition, over 6000 appointments nationwide were rescheduled.[3] At least 1% of all diagnostic equipment was compromised by WannaCry.[3] This caused delays in testing and results, as well as cancellation of numerous appointments in primary care. In total, 31% of secondary care health-care organizations and 8% of primary-care organizations in England were disrupted.[3]

les pouvoirs publics ont accéléré cette tendance, les hôpitaux étant incités à acquérir une plus grande maturité numérique en appliquant des normes industrielles telles que l'échelle d'évaluation EMRAM (Electronic Medical Record Adoption Model) de l'HIMSS.[24]

Suite au remplacement des dossiers sur support papier, les établissements de santé sont désormais tributaires de chaînes d'approvisionnement complexes et dispersées de fournisseurs de matériel et de logiciels pour gérer leurs écosystèmes numériques. Ils sont également confrontés à de nouvelles complexités, telles que l'utilisation d'applications dans le «cloud», le télétravail et l'adoption de l'intelligence artificielle en tant qu'outil d'aide à la prise de décision clinique. Cette plus grande maturité numérique ne s'est pas accompagnée d'un niveau équivalent d'investissement ou de renforcement de la maturité en matière de cybersécurité. Ce fossé entre la maturité numérique et la maturité en matière de cybersécurité a rendu les établissements de santé fortement dépendants des flux de travail numériques, ce qui implique également une certaine vulnérabilité. Les établissements de santé ne disposent souvent pas de suffisamment de visibilité sur la vaste gamme de technologies qu'ils utilisent, sur leur degré de vulnérabilité et sur les conséquences qu'aurait une compromission du système pour la sécurité des patients. Ces circonstances, conjuguées à un manque de leadership et de spécialistes en matière de sécurité dans l'ensemble du secteur, créent de nombreuses opportunités de cibler et de compromettre les établissements de santé.

## Quel est l'impact des rançongiciels sur les résultats sanitaires?

L'impact des attaques par rançongiciel est souvent évoqué en termes financiers. On sait par exemple qu'aux États-Unis d'Amérique, la rançon moyenne payée pour une attaque est supérieure à 100 000 dollars et le coût global de rétablissement des activités dépasse 1 million de dollars.[8] L'attaque par rançongiciel dont a été victime le HSE a coûté plus de 100 millions d'euros aux contribuables irlandais.[25] Cependant, ces considérations financières ne reflètent pas les risques cliniques associés aux attaques par rançongiciel, ni leur impact sur la santé publique.

Pour mieux comprendre ces éléments, il est utile de revenir sur les 2 attaques les plus massives observées à ce jour. L'attaque WannaCry menée contre le NHS a contraint 5 établissements de soins aigus à détourner des ambulances vers d'autres centres pendant 3 jours et a confronté de nombreux établissements à des problèmes d'indisponibilité des services d'imagerie diagnostique. En outre, plus de 6000 rendez-vous ont dû être reportés à l'échelle nationale.[3] Au moins 1% de tout le matériel de diagnostic a été compromis par WannaCry,[3] ce qui a entraîné des retards dans la réalisation des tests et l'obtention des résultats et a conduit à l'annulation de nombreuses consultations en soins primaires. Au total, 31% des établissements de soins secondaires et 8% des établissements de soins primaires ont subi des perturbations en Angleterre.[3]

[24] Electronic Medical Record Adoption Model (EMRAM). Chicago (IL): Healthcare Information and Management Systems Society; 2022 (https://www.himss.org/what-we-do-solutions/digital-health-transformation/maturity-models/electronic-medical-record-adoption-model-emram).

[25] O'Donovan B. HSE cyber-attack cost hits €43m, could rise to €100m. Raidió Teilifís Éireann, 23 February 2022 (https://www.rte.ie/news/ireland/2022/0223/1282617-cyber-attack-cost/).

[24] Electronic Medical Record Adoption Model (EMRAM). Chicago (IL): Healthcare Information and Management Systems Society; 2022 (https://www.himss.org/what-we-do-solutions/digital-health-transformation/maturity-models/electronic-medical-record-adoption-model-emram).

[25] O'Donovan B. HSE cyber-attack cost hits €43m, could rise to €100m. Raidió Teilifís Éireann, 23 February 2022 (https://www.rte.ie/news/ireland/2022/0223/1282617-cyber-attack-cost/).

The HSE's Post Incident Review into the more recent Conti ransomware attack found similar outcomes: 57% of acute hospitals had to cancel appointments and clinical services, including elective surgery, diagnostic imaging, pathology, outpatient appointments and cancer care.[16] The report specifically cited a heightened risk of error as staff switched to paper-based processes for patient identification and processing. The national medical imaging system was also rendered unavailable due to the attack. Examples were cited of oncology patients' treatment cycles being delayed because patient imaging and radiotherapy treatment plans were inaccessible.[16]

More rarely, ransomware attacks were investigated because of an alleged association with patient mortality. In 2020, in Germany, an ambulance carrying a patient had to be diverted from Dusseldorf University Hospital, which was experiencing a ransomware attack. The patient subsequently died. The incident was initially investigated as negligent homicide, the delay in treatment being considered a factor in the death. This line of enquiry was ultimately dropped, as the patient was considered to be in such an adverse state that faster treatment would not have materially improved their outcome.[26, 27] The delay was nevertheless significant enough to warrant investigation and also raised the question of how best to investigate the impact of delayed care on patient populations due to cyber-attacks.

## Discussion

Ransomware has emerged as the leading type of digital DE in health care in less than a decade. The COVID-19 pandemic accelerated this trend, as health-care organizations globally embraced digital transformation to optimize their clinical workflow and provide remote consultations for their patients.

We are now at a point at which the scale of attacks can consistently compromise national critical infrastructure and therefore national security. The misuse of information technology is already a cause for concern for United Nations (UN) Member States and is being analysed by the UN General Assembly Open Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security.[28] More consideration could now be given both through this and complementary frameworks to

Après l'attaque plus récente menée contre le HSE à l'aide du rançongiciel Conti, l'examen post-incident a donné des résultats similaires, indiquant que 57% des hôpitaux de soins aigus ont dû annuler des rendez-vous et des services cliniques, y compris mais non exclusivement dans les domaines suivants: chirurgie élective, imagerie diagnostique, pathologie, consultations ambulatoires et soins contre le cancer.[16] Le rapport a spécifiquement fait état d'un risque accru d'erreurs lié au fait que le personnel a dû recourir à des processus papier pour l'identification et le traitement des patients. L'attaque a également rendu le système national d'imagerie médicale indisponible. Le rapport évoque en outre des cas de patients en oncologie dont les cycles de traitement ont été retardés en raison de l'inaccessibilité de leurs résultats d'imagerie et de leurs plans de traitement de radiothérapie.[16]

Dans des cas beaucoup plus rares, des enquêtes ont été menées pour déterminer s'il existait un lien entre des attaques par rançongiciel et des décès de patients. En 2020, en Allemagne, une ambulance transportant un patient a dû être détournée de l'hôpital universitaire de Düsseldorf, qui subissait une attaque par rançongiciel. Le patient est décédé par la suite, et une enquête a initialement été menée pour homicide par négligence, dans la mesure où le retard dans le traitement pouvait être considéré comme un facteur ayant contribué au décès. Cette piste a finalement été abandonnée, car il a été estimé que le patient était dans un état si grave qu'un traitement plus rapide n'aurait pas sensiblement amélioré ses chances de survie.[26, 27] Toutefois, le retard était de toute évidence suffisamment important pour justifier une enquête et l'incident a suscité une réflexion sur les meilleurs moyens d'évaluer l'impact des retards de soins dus aux cyberattaques sur les patients.

## Discussion

En moins d'une décennie, les attaques par rançongiciel se sont hissées au premier rang des menaces numériques dans le secteur de la santé. La pandémie de COVID-19 a accéléré cette tendance, les établissements de santé du monde entier ayant fait le choix de la transformation numérique pour optimiser leurs flux de travail cliniques et proposer des consultations à distance à leurs patients.

Ces attaques sont aujourd'hui d'une telle ampleur qu'elles risquent régulièrement de compromettre les infrastructures nationales essentielles et, par conséquent, la sécurité nationale. L'utilisation abusive des technologies de l'information est déjà un sujet de préoccupation pour les États Membres des Nations Unies, la question étant abordée par le Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale dans le cadre de l'Assemblée générale des Nations Unies.[28] Il serait désormais opportun, dans ce cadre et dans des

[26] Schneier B. On that Dusseldorf hospital ransomware attack and the resultant death. Schneier on Security, 24 November 2020 (https://www.schneier.com/blog/archives/2020/11/on-that-dusseldorf-hospital-ransomware-attack-and-the-resultant-death.html).

[27] Collier K. Baby died because of ransomware attack on hospital, suit says. NBC News, 30 September 2021 (https://www.nbcnews.com/news/baby-died-due-ransomware-attack-hospital-suit-claims-rcna2465).

[28] Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final Substantive Report. United Nations General Assembly. New York: United Nations; 2021 (https://dig.watch/wp-content/uploads/2022/08/OEWG-Report.pdf).

[26] Schneier B. On that Dusseldorf hospital ransomware attack and the resultant death. Schneier on Security, 24 November 2020 (https://www.schneier.com/blog/archives/2020/11/on-that-dusseldorf-hospital-ransomware-attack-and-the-resultant-death.html).

[27] Collier K. Baby died because of ransomware attack on hospital, suit says. NBC News, 30 September 2021 (https://www.nbcnews.com/news/baby-died-due-ransomware-attack-hospital-suit-claims-rcna2465).

[28] Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final Substantive Report. United Nations General Assembly. New York: United Nations; 2021 (https://dig.watch/wp-content/uploads/2022/08/OEWG-Report.pdf).

addressing the specific threats and ramifications to public health that ransomware and similarly disruptive cyber-attacks pose.

Although there are no data on the precise impact on clinical outcomes, there are compelling data on the scale of disruption to acute services. Diagnostic imaging, pathology, emergency departments, ambulance services and cancer care have all been consistently compromised by ransomware attacks throughout the world. It is likely that not only will the frequency of these attacks continue to increase but also the scale, sophistication and severity of attacks will continue to evolve.

To address this growing digital risk to public health, recommendations should be considered for 5 parameters:

### i. Perception

Practical capability-building is important, as is addressing any perception that cyber-attacks cause only technical problems. Cyber-attacks should be positioned as significant, scalable threats with human consequences. One consideration might be to frame ransomware attacks with language similar to that used to discuss DEs in the context of chemical, biological or radionuclear attacks. The physical destruction of health-care facilities is already considered a war crime by the International Criminal Court, and emergency preparedness teams plan for loss of access to health care or related supply chains. As the outcomes of digital attacks are nearly identical, they could rationally be described in a similar way. A more formal recommendation that could be tested would be extension of the nomenclature for chemical, biological, radiological and nuclear incidents to include disruptive cyber-attacks.

### ii. People

A shortage of cybersecurity professionals has been reported in many sectors. This is particularly acute in health care due to the often limited availability of resources to compensate cybersecurity professionals when compared with sectors such as financial services.

Public health agencies and health-care organizations, with their growing use of digital systems for emergency preparedness, might therefore consider upgrading the skills of their IT and biomedical engineering workforces to ensure appropriate competence for cybersecurity. This could be achieved through several industry standards and certifications (e.g. cybersecurity standards issued by the International Organization for Standardization). It will also be important to create awareness at executive levels of the importance of cyber-attacks as a source of public health emergencies, as this will increase cyber-awareness at all staffing levels. The best way to achieve this would be to appoint a chief informa-

structures complémentaires, d'accorder une plus grande attention aux menaces spécifiques posées par les rançongiciels et les cyberattaques perturbatrices analogues, ainsi qu'à leurs répercussions sur la santé publique.

Bien qu'on manque de données pour décrire l'impact précis de ces attaques sur les conséquences cliniques, on dispose d'informations convaincantes concernant l'ampleur des perturbations subies par les services de soins aigus. Dans le monde entier, des services d'imagerie diagnostique, de pathologie, de soins d'urgence, d'ambulance et de soins contre le cancer sont régulièrement compromis par des attaques par rançongiciel. Il est probable que ces attaques deviendront non seulement plus fréquentes, mais aussi qu'elles seront menées à plus grande échelle et gagneront en complexité et en gravité.

Face à ce risque numérique croissant pour la santé publique, des recommandations peuvent être formulées selon 5 axes différents:

### i. Perception

Outre le renforcement des capacités pratiques, il est important de dissiper toute perception selon laquelle les cyberattaques n'entraînent que des problèmes techniques. Les cyberattaques devraient au contraire être présentées et comprises comme des menaces importantes et évolutives qui ont des conséquences humaines. L'une des possibilités serait de parler des attaques par rançongiciel en employant un langage similaire à celui utilisé pour les actes délibérés commis dans le contexte d'attaques chimiques, biologiques ou radionucléaires. L'attaque physique d'établissements de santé est déjà considérée comme un crime de guerre par la Cour pénale internationale (CPI) et la perte de l'accès aux soins de santé ou aux chaînes d'approvisionnement connexes sont des problèmes que les équipes de préparation aux situations d'urgence anticipent activement. Il est donc logique de décrire les attaques numériques de manière similaire, étant donné qu'elles ont des effets pratiquement identiques. On pourrait envisager une recommandation plus formelle qui consisterait à étendre la dénomination des incidents chimiques, biologiques, radiologiques et nucléaires (CBRN) en y ajoutant les cyberattaques perturbatrices (CBRN c).

### ii. Ressources humaines

Il est largement reconnu que de nombreux secteurs souffrent d'une pénurie de professionnels de la cybersécurité. Ce problème est particulièrement aigu dans le secteur de la santé où, par rapport à d'autres secteurs tels que les services financiers, les ressources nécessaires à la rémunération des professionnels de la cybersécurité sont souvent limitées.

Compte tenu de l'utilisation croissante des systèmes numériques pour la préparation aux situations d'urgence et la prestation des soins de santé, il serait donc utile que les organismes de santé publique mettent l'accent sur le développement professionnel des personnels existants, qu'il s'agisse de spécialistes en informatique ou en génie biomédical, afin qu'ils acquièrent un niveau de compétence adéquat dans le domaine de la cybersécurité. Pour ce faire, on peut s'appuyer sur plusieurs normes et certifications industrielles (par exemple, les normes de cybersécurité de l'Organisation internationale de normalisation). Il est également essentiel de sensibiliser les dirigeants et décideurs à la menace que représentent les cyberattaques et au fait qu'elles peuvent conduire à des

tion security officer who reports directly and regularly to the executive leadership about ongoing risks, how they are being mitigated and the resources required for appropriate remediation.

Such investments in people are essential to maximize the benefits that can be derived from more significant investments in cybersecurity, such as the development of security operations centres and enhanced collaboration with national cybersecurity capabilities such as computer security incident response teams (CSIRTs).

### iii. Processes

Given the clinical disruption caused by ransomware attacks, processes should be developed to mitigate their impact. Such actions should be considered in the context of a prevention – detection – response – recovery cycle.

Prevention and detection are the elements that receive the most attention, as many cybersecurity solutions address them. Less attention has been paid to development of resilience and rehearsal of incident response and recovery processes, such as in planning for natural disasters or terrorist events. It is recommended therefore that public health agencies develop guidance on clinical incident response planning that specifically addresses how health-care organizations should respond to disruptive cyber-attacks such as ransomware.

The guidance may include:

- training clinical staff to transition to downtime processes to maintain a baseline level of clinical service quality during a ransomware attack;
- establishing clear communication pathways with suppliers of digital systems, government agencies, computer emergency response teams (CERTs) and CSIRTs, and law enforcement and criminal justice systems to report incidents and request support; and
- establishing a regularly updated, local, offline back-up of critical information and systems for effective recovery from a ransomware attack.

### iv. Technology

A wide range of cybersecurity products and managed services are available directly in the private sector and, in some instances, are subsidized by government agencies that address prevention and detection. Given the relatively nascent maturity of health-care organizations with respect to cybersecurity, 2 areas should be considered.

urgences de santé publique; cela favorisera une meilleure compréhension des enjeux de la cybersécurité à tous les niveaux des organisations. Le meilleur moyen d'atteindre cet objectif est de nommer un responsable de la sécurité de l'information qui rende compte directement à la direction et qui l'informe régulièrement des risques en cours, des mesures prises pour les atténuer et des ressources nécessaires pour y remédier de manière adéquate.

Ces investissements dans les ressources humaines sont indispensables pour tirer le meilleur parti possible d'autres investissements plus conséquents dans la cybersécurité, tels que la mise en place de centres des opérations de sécurité. Ils favoriseront en outre une meilleure collaboration avec les entités nationales de cybersécurité, comme les équipes d'intervention en cas d'incident de sécurité informatique (CSIRT, Computer Security Incident Response Team).

### iii. Processus

Compte tenu des conséquences cliniques engendrées par les attaques par rançongiciel, il est indispensable de mettre en place des processus susceptibles d'en atténuer l'impact. Ces actions doivent s'inscrire dans le cadre d'un cycle «Prévention – Détection – Intervention – Rétablissement».

La prévention et la détection sont les éléments qui sont les mieux pris en compte, car il existe de nombreuses solutions de cybersécurité axées sur ces objectifs. On accorde généralement moins d'attention aux mesures destinées à renforcer la résilience et à simuler les processus d'intervention et de rétablissement en cas d'incident, comme on le ferait dans le cadre de la préparation aux catastrophes naturelles ou aux actes de terrorisme. Il est donc recommandé aux organismes de santé publique d'élaborer des «lignes directrices pour la planification des interventions en cas d'incident clinique», qui traitent spécifiquement de la réponse que les établissements de santé doivent apporter aux cyberattaques perturbatrices telles que celles menées par rançongiciel.

Ces lignes directrices peuvent inclure les conseils suivants:

- Former le personnel clinique pour qu'il sache quels processus adopter en cas d'arrêt des systèmes informatiques de sorte à maintenir un niveau de qualité de base des services cliniques lors d'une attaque par rançongiciel.
- Établir des voies de communication claires avec les fournisseurs de systèmes numériques, les organismes publics, les équipes d'intervention en cas d'urgence informatique (CERT, Computer Emergency Response Teams)/CSIRT et les services de police et de justice pénale pour signaler les incidents et demander de l'aide.
- Effectuer une sauvegarde locale, hors connexion et régulièrement actualisée des informations et des systèmes critiques pour permettre une restauration efficace des données après une attaque par rançongiciel.

### iv. Technologies

Il existe une large gamme de produits et de services de cybersécurité, disponibles directement dans le secteur privé ou parfois subventionnés par des organismes publics, qui sont axés sur la prévention et la détection. Compte tenu du niveau de maturité relativement peu avancé des établissements de santé en matière de cybersécurité, 2 domaines particuliers méritent d'être explorés.

The first is to identify technologies and managed services that create greater visibility of digital assets throughout the network of a health-care organization. This should cover traditional IT (for example, desktops, laptops), network infrastructure (for example, servers, security appliances) and medical devices. It will not be possible to mitigate risk effectively without such transparency, which can be achieved through manual cataloguing or automated solutions.

Once digital assets have been identified, solutions and services are available on the market or through national CERT/CSIRT capabilities to identify their vulnerabilities and to quantify the associated risks in both technical and clinical terms. These technologies can be used to rank the assets that present the most severe risks to an organization if exploited and so guide prevention and monitoring activities accordingly.

Many more products and services are available on the market that address prevention and detection, such as threat intelligence, access management, firewall and security orchestration products. It is also possible to outsource some cybersecurity capabilities through managed security service providers; however, the preceding steps are considered the most prudent to be taken initially.

### v. Collaboration

The impact of highly disruptive cyber-attacks such as ransomware necessitates greater multi-disciplinary cooperation to mitigate public health risks. This should go beyond the already emerging relationships between health-care providers and law enforcement agencies.

First, law enforcement, criminal justice institutions (prosecution and judiciary), national security agencies, ministries of health, CERTs/CSIRTs, industry stakeholders and public health bodies could, ideally, form multi-disciplinary national working groups to better understand the disruptive cyber threats they face. Such coordinated, regular communication could generate specific recommendations, which, if appropriately costed, will support the adoption of best practices in preparatory and incident response to preserve patient safety in ransomware attacks. Collaborative actions of this nature to address the rise of ransomware, although not specific to health care, have emerged during the pandemic from INTERPOL, the UN Office on Drugs and Crime (UNODC) and the World Economic Forum.[29]

Secondly, more sharing of intelligence about threats and threat actors that target health-care systems and life sciences supply chains could be encouraged among Member States. This may include facilitation of infor-

[29] Immediate action required to avoid ransomware pandemic. Lyon: INTERPOL; 2021 (https://www.interpol.int/en/News-and-Events/News/2021/Immediate-action-required-to-avoid-Ransomware-pandemic-INTERPOL).

Le premier consiste à identifier les technologies et les services qui permettent d'obtenir une meilleure visibilité des actifs numériques dont dispose un établissement de santé sur l'ensemble de son réseau. Parmi ces actifs figurent le matériel informatique traditionnel (p. ex., ordinateurs de bureau, ordinateurs portables), l'infrastructure réseau (p. ex., serveurs, dispositifs de sécurité) et les dispositifs médicaux. Il n'est pas possible d'atténuer efficacement les risques sans disposer de cette visibilité, qui implique de procéder à un catalogage manuel ou d'utiliser des solutions automatisées.

Une fois les actifs numériques recensés, il existe des solutions et des services, disponibles sur le marché ou par le biais des équipes CERT/CSIRT nationales, qui permettent d'identifier les vulnérabilités de ces actifs et de quantifier les risques associés, tant sur le plan technique que clinique. Ces technologies peuvent être utilisées pour classer les actifs qui présentent les plus grands risques pour une organisation en cas d'attaque et ainsi orienter les efforts de prévention et de surveillance en conséquence.

De nombreux autres produits et services sont proposés sur le marché pour la prévention et la détection, tels que les produits de renseignement sur les menaces, de gestion des accès, de pare-feu et d'orchestration de la sécurité. Il est également possible d'externaliser une partie des capacités de cybersécurité auprès de prestataires de services gérés de sécurité. Cependant, il est plus prudent de commencer par prendre les mesures décrites ci-dessus.

### v. Collaboration

Compte tenu des fortes perturbations occasionnées par les cyberattaques, notamment les attaques par rançongiciel, une plus grande coopération multidisciplinaire est nécessaire pour atténuer les risques qu'elles posent pour la santé publique. Cette collaboration va au-delà de la relation déjà amorcée entre les prestataires de santé et les autorités policières.

Premièrement, l'idéal serait que les services de police, les institutions de justice pénale (ministère public et appareil judiciaire), les organismes de sécurité nationale, les ministères de la santé, les équipes CERT/CSIRT, les partenaires industriels et les organismes de santé publique forment des groupes de travail nationaux multidisciplinaires visant à mieux cerner les cybermenaces perturbatrices auxquelles ils sont confrontés. Une communication régulière et coordonnée de ce type peut aboutir à des recommandations concrètes qui, sous réserve d'une évaluation adéquate des coûts, favoriseront l'adoption de meilleures pratiques de préparation et de riposte aux incidents, ce qui contribuera à protéger la sécurité des patients en cas d'attaque par rançongiciel. Face à la recrudescence des attaques par rançongiciel, des actions collaboratives de cette nature, bien que non spécifiques au secteur de la santé, ont vu le jour pendant la pandémie sous l'impulsion d'INTERPOL, de l'Office des Nations Unies contre la drogue et le crime (ONUDC) et du Forum économique mondial.[29]

Deuxièmement, il convient d'encourager les États Membres à partager davantage d'information, de type «renseignement» sur les menaces et les acteurs qui ciblent les systèmes de santé et les chaînes d'approvisionnement dans le domaine des sciences

[29] Immediate action required to avoid ransomware pandemic. Lyon: INTERPOL; 2021 (https://www.interpol.int/en/News-and-Events/News/2021/Immediate-action-required-to-avoid-Ransomware-pandemic-INTERPOL).

mation- and intelligence-sharing by private sector cybersecurity companies, non-profit organisations, defence contractors or international networks of incident response teams such as the Forum of Incident Response and Security Teams, as well as neutral intergovernmental law enforcement platforms such as INTERPOL. This will be necessary to identify emerging risks that present national and cross-border security threats. As health-care technology supply chains are extensively interconnected globally, this type of collaboration could mitigate the contagion effects that can occur through ransomware attacks on major technology suppliers.

Thirdly, Member States could consider creating common cybersecurity capabilities that are globally accessible. One example would be to work with the UN International Computing Centre, which has previously developed common cybersecurity capabilities for institutions within the UN system.

Finally, global intergovernmental agencies such as WHO, other UN agencies and INTERPOL could consider a formal definition of public harm in the context of disruptive cyber-attacks such as ransomware. This could be explored in forums such as the aforementioned UN OEWG or through broader emerging UN conventions addressing cyber-crime, such as the "Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes", led by Member States, for which the UNODC is the secretariat.[30]


## Acknowledgements

John Billow, INTERPOL, Singapore; Sylvie Briand, WHO, Geneva, Switzerland; Carmen Corbin, UNODC, Dakar, Senegal; Akvile Giniotiene, UNOCT, New York, USA; Victoria Haldane, WHO, Geneva, Switzerland; Matthew Lim, US Department of Health and Human Services, Geneva, Switzerland; Charlotte Lindsey, CyberPeace Institute, Geneva, Switzerland; Orhan Osmani, International Telecommunications Union, Geneva, Switzerland; Maria Rettori, UNOCT, New York, USA; Tima Soni, UNICC, Valencia, Spain.



## Author affiliations

[a] Biosecurity and Health Security Protection Unit, Epidemic and Pandemic Preparedness and Prevention Department, WHO Health Emergencies Programme, WHO, Geneva, Switzerland (corresponding author: Dr Nahoko Shindo, shindon@who.int).


[30] Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. Vienna: United Nations Office on Drugs and Crime; 2022 (https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home).

de la vie. Cet échange d'informations et de renseignements pourra notamment être facilité par des entreprises de cybersécurité privées, des organisations non gouvernementales et des sociétés du secteur de la défense, des réseaux internationaux regroupant des équipes d'intervention en cas d'incident comme FIRST (Forum of Incident Response and Security Teams), ou encore des plateformes policières intergouvernementales telles qu'INTERPOL. Ce partage sera indispensable pour identifier les risques émergents qui constituent des menaces pour la sécurité tant à l'échelle nationale qu'au niveau transfrontalier. Étant donné que les chaînes d'approvisionnement des technologies de santé sont fortement interconnectées à l'échelle mondiale, ce type de collaboration peut contribuer à atténuer les effets de contagion qui pourraient résulter d'attaques par rançongiciel menées contre certains grands fournisseurs.

Troisièmement, les États Membres peuvent envisager d'établir des capacités communes de cybersécurité accessibles à l'échelle mondiale. Cela pourrait par exemple passer par une collaboration avec le Centre international de calcul des Nations Unies (CIC), qui a déjà développé des capacités communes de cybersécurité pour les institutions du système des Nations Unies.

Enfin, des organismes intergouvernementaux mondiaux tels que l'OMS, d'autres agences onusiennes et INTERPOL pourraient réfléchir à la définition officielle devant être donnée à l'expression «préjudice public» dans le contexte de cyberattaques perturbatrices telles que les attaques par rançongiciel. Cette question peut être abordée au sein de forums tels que le Groupe de travail à composition non limitée susmentionné ou dans le cadre des nouvelles conventions plus générales des Nations Unies sur la cybercriminalité, telles que la «Convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles», dont l'élaboration est dirigée par les États Membres et dont le Secrétariat est assuré par l'ONUDC.[30]


## Remerciements

John Billow, Organisation internationale de police criminelle (INTERPOL), Singapour; Sylvie Briand, Organisation mondiale de la Santé (OMS), Genève (Suisse); Carmen Corbin, Office des Nations Unies contre la drogue et le crime (ONUDC), Dakar (Sénégal); Akvile Giniotiene, Bureau de lutte contre le terrorisme (BLT) des Nations Unies, New York (États-Unis d'Amérique); Victoria Haldane, OMS, Genève (Suisse); Matthew Lim, Département de la Santé et des Services sociaux des États-Unis, Genève (Suisse); Charlotte Lindsey, CyberPeace Institute, Genève (Suisse); Orhan Osmani, Union internationale des télécommunications des Nations Unies, Genève (Suisse); Maria Rettori, BLT, New York (États-Unis d'Amérique); Tima Soni, Centre international de calcul des Nations Unies (CIC), Valence (Espagne).



## Affiliations des auteurs

[a] Unité Biosécurité et protection de la sécurité sanitaire, Département Prévention et préparation aux épidémies et pandémies, Programme OMS de gestion des situations d'urgence sanitaire, OMS, Genève (Suisse) (auteur correspondant: Dr Nahoko Shindo, shindon@who.int).


[30] Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. Vienna: United Nations Office on Drugs and Crime; 2022 (https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home).