Analytical Insight

worldbank.org/digitaldevelopment

WORLD BANK GROUP
Digital Development

July 2020

HOW COVID-19 HAS EXPOSED CYBER RISKS IN THE HEALTH SECTOR

Why a Paradigm Shift is needed for Building Cybersecurity Resilience

Key Findings

- Cyberattacks targeting public health and the health sector have increased significantly since the outbreak of the COVID-19 pandemic in 2020, resulting in disruption to the operations of domestic healthcare systems and services, theft of medical records, and significant financial losses, elevating the need to bring cybersecurity to the forefront of the development agenda.
- Low preparedness – resulting from insufficient cybersecurity investment and awareness in developing countries generally and from the unprecedented challenges presented by a pandemic specifically – renders low- and medium-income countries particularly at risk of paralyzing attacks.
- A sectoral-centered approach is needed to bolster cybersecurity within the health domain, using the historically strong development of cybersecurity in the financial sector to offer lessons to fortify the health sector against threats. This sectoral capacity building must be anchored to a strong foundation and enabling environment provided by a central national cybersecurity agency whose capacity must also be built and fortified to support the health sector.
- A broad conceptualization of cybersecurity to include elements of malicious information campaigns will help facilitate a focus and better management of this rapidly developing phenomenon.
- The COVID-19 pandemic has underscored the need to establish cybersecurity as a core element of the digital development agenda in the 21st century, and yields a unique clarity and opportunity to accelerate the safe and effective development and adoption of e-health solutions and telehealth platforms, particularly in low- and middle-income countries – paving the way towards further digital development of the health sector.

CYBERATTACKS DURING COVID-19

While much of the discourse on cybercrimes and cyberattacks during COVID-19 has focused on individuals, businesses, and government agencies more generally, the narrower domain of public health and the health sector has experienced an exponential increase in attacks during this same time period. This has demanded a greater analytical assessment to inform a re-calibrated response where necessary. Cyber criminals have exploited the circumstances of the pandemic during a time when digital connectivity, reliance on digital applications, and an urgent demand for information about confronting the virus are at an all-time high. The health sector was an early target, experiencing a 150% increase in cyberattacks in the first two months of 2020,[1] including a significant uptick in attacks against hospital infrastructure in particular.[2] This compounded what was already an increasing trend of cyberattacks in the health sector, which in 2019 had a 60% increase in threat detections amongst healthcare organizations in the United States alone.[3] While historically many of these attacks against the health sector were focused on gaining access to public health records and personally identifiable information, the targets and objectives have now diversified more broadly to also include attacks against vaccine research institutions as well as misinformation campaigns around public health messages.[4] Significantly more investment and sectoral focus is needed to raise awareness and build cybersecurity capacity, particularly in developing countries. The experience of COVID-19 has accelerated the need to elevate cybersecurity as a core component of the development agenda and precipitated a unique opportunity to do so.

FIVE MOST COMMON FORMS OF MALICIOUS CYBER ACTIVITY TARGETING THE HEALTH SECTOR DURING COVID-19

In order to understand the relationship between targets and risks in the Health sector during COVID-19, it is important to review a basic taxonomy of the types and forms of cyberattacks, including their technical characteristics, purpose, and objectives.[5] While there are many types of cyberattacks, the list below distills this broader catalog down to the most common forms of malicious cyber activity that have targeted public health and the health sector during the COVID-19 pandemic, including malware, phishing, ransomware, denial-of-service attacks, and various types of malicious information-related campaigns.[6] [7] [8] [9] [10] [11]

TYPE OF ATTACK	DEFINITION
Malware	A form of malicious code that is designed to damage or disrupt a computer system, or to gain unauthorized access into a system. Malware can manifest in a variety of form, the most common being viruses, worms, Trojan horses, and spyware.
Phishing & Spear Phishing	An attempt by perpetrator to acquire sensitive data through fraudulent solicitation - most often using emails and websites. Spear phishing is a more targetted version of phishing that involves well-researched victims, social engineering, and personalized messages to gain trust.
Ransomware	A type of malware intented to block access to a computer system, files, or data until a ransom is paid
Denial-of-Service (DoS) & Distributed Denial-of-Services (DDoS)	Prevent authorized access to resources and content for a certain amount of time. For certain time-critical operations - which are ubiquitous throughout healthcare - even a delay lasting milliseconds can yield significant damage.
Malicious Information Campaigns	- **Misinformation:** Information that is false but not created with the intention of causing harm. - **Disinformation:** False information that is intentionally used to cause harm. - **Mal-information:** Information based on reality that is used to cause harm.

TOP FIVE TRENDS REGARDING TARGETS FOR CYBERATTACKS IN THE HEALTH SECTOR

The five most common targets of cyberattacks in the health sector during the COVID-19 pandemic have been hospitals and health centers, domestic and international public health organizations, vaccine companies and research institutions, individuals, and contact tracing apps. Each of these targets is associated with a distinct set of risks and vulnerabilities, as described below:

Trending Target #1: Hospitals & health centers

Hospitals and health centers including their computer systems, infrastructure, and healthcare workers have been a top target for cyberattacks, with criminals exploiting weak security systems and architecture, according to Interpol.[12] This has led the international policing agency to issue a 'Purple Notice'[13] warning to police in 194 countries about the increasing threat to healthcare facilities during COVID-19.[14] The fact that these healthcare facilities are also filled with ill and vulnerable patients whose health conditions may be dependent upon digitally-enabled treatment and care makes them a prime target for ransomware in particular. With a heightened stress environment caused by the pandemic, hospital dependency on uninterrupted digital connectivity renders their staff more likely to accept the conditions of ransomware in order to avoid the potentially lethal consequences of not complying with a cyber criminal's request. A lack of dedicated cybersecurity staff along with absent training and awareness amongst hospital staff on cyber resilient behaviors further exacerbates this phenomenon. This so-called 'insider threat' has been further amplified in some countries like the United Kingdom, where there has been extensive hiring of temporary staff, including a re-hiring of retired workers, to meet the demands of the pandemic. Even experienced health workers can lack awareness of the latest cyber risks in the health sector, particularly risks associated with the increased use of remote consultations and tele-health platforms. In just the first few months of the COVID-19 pandemic countries all over the world experienced attacks on their hospitals' and health centers' digital assets, including France, Spain, Thailand, and the United States.[15]

BOX 1: CYBERATTACK AGAINST HOSPITAL IN CZECH REPUBLIC

On March 13, 2020 the Brno University Hospital ¬in the Czech Republic was hit by a cyberattack, threatening not only the lives of patients inside, but also the country's broader pandemic response due to its containment of one of the country's largest COVID-19 testing laboratories. The ransomware forced staff at the hospital to shut down their digital network, cancel scheduled surgeries, and transfer patients to other hospitals. As dangerous as this attack was, its relatively early timing during the global pandemic undoubtedly served as a warning to act for other hospitals and health centers with significant cyber vulnerabilities – both within the Czech Republic, and across the globe.

Source 1: Ruhl, C. 2020. "Note to Nations: Stop Hacking Hospitals." Foreign Policy. April 6. See https://foreignpolicy.com/2020/04/06/coronavirus-cyberattack-stop-hacking-hospitals-cyber-norms/

Source 2: Cimpanu, C. and Z. Day. 2020. "Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak." ZD Net. March 13. See https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/

Trending Target #2: International & domestic public health organizations

Internationaland domestic public health institutions and organizations have also been focal points of attacks. The World Health Organization (WHO) is the most prominent international health institution that has been targeted, with attack attempts increasing by 500% over the same period in the year prior to the COVID-19 pandemic.[16] Email addresses and passwords of staff members have been leaked online following successful attacks.[17] The United States has experienced attacks at the national and regional levels, with the US Department of Health and Human Services experiencing a sharp increase in DDoS attacks,[18] while the Champaign-Urbana Public Health District in Illinois was attacked with ransomware.[19] Though data that was stored on cloud servers was not breached in Champaign-Urbana, the ransomware did manage to block access to files for staff for a period. Cyber criminals have also exploited the trusted reputations and brands of prominent public health agencies by referencing them in the subject lines of emails and the URLs of fraudulent or malicious websites.

Trending Target #3: Vaccine companies, research institutions, & bio-tech businessess

This category refers to organizations primarily involved in vaccine research, which includes universities, publicly administered organizations, private companies, and public-private partnership ventures. Criminals in this group are often thought to be supported by nation-states aiming to gain a lead in finding a vaccine, though publicly available support for these claims are difficult to verify or assess.[20] In July 2020 the United Kingdom's National Cyber Security Centre (NCSC) announced a major malware attack dubbed APT29 against organizations involved with vaccine research in the United Kingdom, the United States, and Canada, with the likely aim of 'stealing information and intellectual property relating to the development and testing of COVID-19 vaccines'.[21] Another example of a such an attack includes the Hammersmith Medicines Research organization, a British medical facility that was on standby to assist with coronavirus vaccine testing, having previously been involved with testing for an Ebola vaccine.[22] While research findings and patented intellectual property for pharmaceutical drugs and vaccines have long been a target of attack prior to the pandemic for both commercial entities and nation-states to gain a competitive edge, COVID-19 has broadened the focus of this criminal activity to not just coronavirus vaccines but also treatment drugs.[23]

Trending Target #4: Individuals

While individuals have always been targets for cybercrime, the significant increase in the amount of time spent interfacing with digital platforms through telework and e-learning content has concomitantly

raised their exposure to potential cyberattacks, particularly malware and malicious information campaigns. Anxiety around the pandemic has been exploited by cyber criminals, who have disguised phishing emails as being sent from reputable organizations such as the WHO, Johns Hopkins University, or the U.S. Center for Disease Control (CDC), or referenced these institutions in email subject lines or file attachments to prompt the downloading of malicious code. In one week alone in April 2020, Google's Gmail service identified 18 million daily malware and phishing emails related to COVID-19, combined with another 240 million daily COVID-19 related spam messages.[24] Promises of COVID-19 cures, health advice, or updated situational reports and tracking maps have also been used to trick individuals into various forms of cyberattacks.[25] For example, malicious websites have been developed that mimic the ubiquitous and oft-cited Johns Hopkins University COVID-19 case map, infecting site visitors with information-stealing trojan type viruses.[26] More sophisticated forms of malware have been deployed through common telework platforms used by health sector employees working from home, most notably through virtual private-network (VPN) applications and popular productivity applications.

Another occurrence that has been observed in this category during COVID-19 has been malicious code intended only to destroy files rather than facilitate financial gain on the part of the attacker; it remains unclear to what extent these type of attacks lacking financial gain were merely deployed as tests for future attacks, or for other reasons.[27] Other forms of cyberattacks against individuals have been in the form of malicious information campaigns regarding virus source, prevention, symptoms, diagnosis, and treatment of COVID-19 in order to create confusion and distrust amongst people and institutions, as well as cause actual harm.[28] This has led to mass-poisonings in Iran and Nigeria and even deaths in USA from the ingestion of cleaning products to overdoses of non-proven treatment drugs like hydroxychloroquine.[29]

Trending Target #5: Contact tracing Apps

Contact tracing apps may be one of the more innovative tools for flattening the curve for infections, but they come with considerable risk due to varying degrees of exposure to cyber criminals. These apps have been deployed through both mobile platforms and websites, and have been developed in very different time periods, with later apps benefiting from additional lessons about possible vulnerabilities in earlier deployed data and system architecture. The utility of these apps relies on the sharing of both location information and personal information – including medical data – to track down individuals who may have had contact with an infected person. In addition, the data from these apps helps inform the development of analytical models that explain behavioral patterns in an infected population, and the development of predictive models used to estimate the statistical likelihood and

location of new infection hotspots. They most often rely on Bluetooth technology to detect proximity between individuals, where one has self-reported a positive infection. Vulnerabilities to information theft manifest at three distinct stages which include the data entry and collection stage, the data sharing stage, and the data storage stage. One of the most notable areas of contention around data storage has been whether it ought to manifest in a decentralized manner on local devices (as proposed jointly by Apple and Google and initially advocated by the Government of Germany), or a local centralized database (as developed by and advocated for by the Government of France and initially the United Kingdom, before the British government decided to switch over to the decentralized model advocated by Google and Apple).[30] [31] Each type of aforementioned data storage architecture has since been designed, and it remains to be seen which will enable the most damaging manipulation and theft of data by cyber criminals.[32]

BOX 2: BACKLASH AGAINST GOVERNMENT-LED CONTACT-TRACING APP IN THE UNITED KINGDOM

On April 29th, 2020, hundreds of scientists and academics from the fields of computer science and information security and privacy and based at British universities signed a petition urging the NHSX unit of the government to reevaluate the benefits of a contact tracing app they were developing against the broader range of costs. These costs included threats to information theft through cyberattacks and security vulnerabilities. This petition was notable due to the expertise, standing, and influence of the signatories, who implored the government to limit the scope of data collection to only what is necessary for the specific task of tracing, and omit other data that is either easy to collect or simply 'nice-to-have'. They also urged the government to ensure no database developed alongside the app that would enable de-anonymization of users who did not self-report being infected. This petition echoed concerns declared in an earlier petition signed by scientists and researchers from around the world and released as a joint statement for all governments considering contact-tracing apps. The government has since published the app's open-source code, and committed to publishing the key security and privacy designs.

Source 1: Soltani, A., Calo, R., and C. Bergstrom. 2020. "Contact-tracing apps are not a solution to the COVID-19 crisis." Brookings Institute. April 27.
See https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/

Source 2: Gould, M. and G. Lewis. 2020. "Digital contact tracing: protecting the NHS and saving lives. NHS Blogs. April 24.
See https://www.nhsx.nhs.uk/blogs/digital-contact-tracing-protecting-nhs-and-saving-lives

THREE GLOBALLY EMERGING THEMES THAT CHALLENGE THE STATUS QUO APPROACH TO CYBERSECURITY

As the first wave of the COVID-19 infections begins to flatten in many countries and the bigger picture of cyber risk in the health sector becomes clearer, three global themes are emerging. These themes challenge the traditional approaches to cybersecurity, and suggest the need for a paradigm shift in how this threat is effectively managed in healthcare and the public health sector in particular.

1 A national approach to developing cybersecurity capacity is no longer sufficient to build the capacity needed in the health sector to protect against cyber-attacks.

COVID-19 has demonstrated that a deeper sectoral-focused approach is now needed, which will not only prioritize this sector and bring it to the forefront, but also help facilitate the tailored solutions needed to protect against such a vast range of threats which includes malware and financially motivated attacks, as well as malicious information campaigns. Here, the successful cyber capacity development in the financial sector in many countries provides a useful template for how governments, health organizations, and other relevant stakeholders can help facilitate a sectoral-focused approach complementary to the development of a national cybersecurity backbone. In order to succeed, this sectoral capacity building must be anchored to a strong foundation and enabling environment provided by a central national cybersecurity agency, along with a mechanism for robust communication and learning between these institutions and other government agencies. A budget and funding mechanism for capacity building in healthcare is also critical for success, as many governments lack the financing that was provided by banks for the finance sector.

2 Malicious information campaigns must be re-conceptualized as core elements of a new cybersecurity regime – particularly within the health sector

– in order to enable governments and other stakeholders including online social media platforms to more effectively manage it. Orchestrated misinformation campaigns have leveraged COVID-19 and broader health-related themes to spread virally through social media to create confusion and distrust amongst people, as well as cause actual harm.[33] False or misleading medical

advice and coronavirus cures have been a particularly common and dangerous phenomena that have spread across the globe at an unprecedented scale, leaving countries struggling to cope. While there are examples of countries like Romania[34] which have attempted to regulate the spreading of malicious information (often dubbed 'fake news' in the policy announcements) by asking telecommunications operators to intervene, or the Philippines[35] which developed a COVID-19 information task force to control and report on instances of it, it is the Israeli classification of disinformation and mal-information which provides a powerful example of action using a limited cyber regulatory mechanism, balanced against the nation's valued freedom of speech principles and democratic norms. While Israel originally limited this regulation to the national election campaign in 2019, this model can be used to design an application for the health sector to enable the government to force online platforms operating within the country to block similar forms of malicious public health information, particularly during pandemics and other public health crises.

BOX 3: ISRAEL'S APPROACH TO CONTROLLING MALICIOUS INFORMATION CAMPAIGNS

While multiple legislative proposals in Israel have called for the inclusion of controls around disinformation and mal-information within cybersecurity regimes, none have been codified into law. However, the Central Election Committee has enabled this conceptualization of cybersecurity to apply to both the April 2019 national election and the September 2019 national election. This electoral sector application was motivated by actual cyber-attacks and foreign intervention against political players, undoubtedly connected to Israel's broader geopolitical situation. These interventions sparked fears of attempts by both domestic and foreign players to spread false or misleading information through online social media platforms intended to sway electoral outcomes. The policy resulted in Facebook and Google taking steps to coordinate compliance around certain types of election-related information. The specific, targeted sectoral scope provides an insightful example of how a similar response for targeting public health can be formulated, even if limited temporally to the period of a public health crisis.

Source: Library of Congress. 2020. "Government Responses to Disinformation on Social Media Platforms: Israel." Legal Library of Congress Reports. Updated March 16.
See https://www.loc.gov/law/help/social-media-disinformation/israel.php

3 **A third emerging theme from the experience of COVID-19 that challenges the traditional uncoordinated approach to cybersecurity is the need to facilitate multi-lateral coordination in capacity building not just at the national level – but on domestic health sectors more specifically.**

There are multiple examples of successful cybersecurity coordination between countries globally in other sectors and domains, such as telecommunications and finance – often to facilitate necessary cross-border transactions. One particular sub-domain within the health sector that will require a similar level of multi-lateral coordination across borders is with contract tracing apps, and their associated data protection policies (health and medical related data at the very least). One model has already been developed for the European market, also known as the Common EU toolbox for Member States, which is a gold-standard for contact tracing app data policies, interoperability standards, and governance guidelines.[36] In practice however, neighboring countries in Western Europe have taken very different approaches to data architecture and managing cyber vulnerabilities, with Germany, Italy, and Denmark applying the peer-to-peer model of distributed data storage on mobile handsets, contrasting sharply with the Government of France which has taken a centralized-database approach for their nationwide COVID-19 app data. As noted earlier the United Kingdom switched between approaches in June 2020, and it remains to be seen whether other countries will also shift their approach towards that of neighboring countries. As these apps are still in development in many countries, it is an opportune time to encourage and facilitate as much regional coordination as possible not just for contact-tracing apps, but other cross-border data flows such as malicious public health information content creation and consumption. This critical need for multi-lateral coordination in app development and data security policies will only grow with time, as these contact-tracing apps will inevitably be used again to manage future waves of COVID-19, as well as other infectious disease outbreaks.

CYBERSECURITY SOLUTIONS FOR THE HEALTH SECTOR

While new themes have emerged challenging the traditional and insufficient approaches to cybersecurity in the health sector, the specific technical solutions for best practices are mostly known and still hold in the case of COVID-19. Here, the greatest impact of the novel coronavirus pandemic in 2020 has been to underscore the importance of these technical best practices and provide further empirical support to expedite cybersecurity awareness and capacity-building programs in national health sectors. These technical solutions include:

- **Establishing and fortifying security operational centers (SOCs) and information sharing and analysis centers (ISACs) for the health sector** to provide centralized information on the latest threats. This also helps coordinate expertise, as well as response support.

- **Implementing health sector-focused vulnerability scans and penetration testing** of hospitals and healthcare centers' digitally connected systems and network infrastructure, including medical machines and devices as well as cloud computing platforms and both mobile and web-based telehealth applications.

- **Designing and implementing health sector-focused awareness campaigns** which include information about general cybersecurity and vulnerabilities for healthcare workers as well as citizens, and also awareness campaigns on how to identify and respond to different types of malicious information campaigns.

- **Integrating best practices around data collection, storage, and sharing by contact tracing apps**, which is narrowly limited to only the data that is needed to achieve the specific objective of contact tracing, and which ensures that anonymized information of non-infected individuals cannot be de-anonymized.

- **Integrating best practices for privacy standards around health and medical data with best practices around data security for Internet of Things (IoT) solutions and 5G-supported cybersecurity networks in the health sector.** This will become increasingly important as telework and telehealth platforms, as well as hospital and health center information and communication infrastructure become increasingly reliant upon these technologies in the coming years.

- **Investing in private sector solutions and forging public-private partnerships with cybersecurity firms to compliment public sector responses.** Governments that already partner with the private sector should seek more tailored solutions for the health sector and create new partnerships with security firms that have a proven track-record with building cyber resilience for this sector.

MAJOR OPPORTUNITY FOR DEFINING CYBERSECURITY AS A CORE DEVELOPMENT OBJECTIVE

For developing countries, including low-and medium-income economies, the COVID-19 pandemic has dramatically underscored the need to prioritize building cybersecurity capacity within the health sector and represents a rare opportunity to establish cybersecurity more broadly as a core element of the 21st Century's development agenda. This further precipitates the need to mobilize the requisite funding mechanisms and multi-lateral coordination needed to facilitate global capacity building and maximize cybersecurity on a global scale so that gaps in the weakest national link of a

digitally-connected network cannot be compromised and exploited to spread further harm throughout globally connected networks. The UN High Level Panel on Digital Cooperation – convened by the Secretary General to provide recommendations on how the international community can work together on cybersecurity issues – is a useful starting point for developing a global framework for cybersecurity coordination.[37] The globally-shared experience of COVID-19 – particularly in terms of cybersecurity risks for all five categories of targets noted in this article – can help fast-track this discussion among the United Nations General Assembly. Other globally coordinating mediums such as multilateral development banks can also be leveraged to ensure cybersecurity capacity building is able to access adequate financing as well as specialist knowledge.

Future healthcare systems and services will increasingly depend on data and advanced digital technologies. Further cybersecurity capacity building of this sector will therefore be required to enable countries, citizens, and healthcare institutions to accelerate the safe adoption and mainstreaming of the latest digitally-enabled healthcare technologies, including not only innovative e-health solutions and telehealth platforms, but also robotic technologies, drones, and IoT devices enabled by 5G networks. With a cyber-resilient environment containing up-to-date cybersecurity solutions and practices within and across public health institutions and the health sector more broadly, the shared experience of COVID-19 provides a unique, clear, and crucially a politically-feasible opportunity to make significant progress towards overcoming critical development challenges around public and individual health and infrastructure objectives.

ACKNOWLEDGMENTS

This article benefited from the contributions of **Natalija Gelvanovska-Garcia**, Senior Digital Development Specialist; **Sandra V. Sargent**, Senior Digital Development Specialist; **Bertram Boie**, Senior Economist; and **Rami Amin**, Consultant.

The authors would like to thank the following colleagues from across the World Bank Group for their review and suggestions: **Anat Lewin**, Senior Digital Development Specialist; and **Jane Treadwell**, Lead Digital Development Specialist.

The authors would also like to thank external peer reviewers including: **Saira Ghafur**, Lead for Digital Health, Institute of Global Health Innovation at Imperial College London.

REFERENCES

[1] Kent, C. 2020. "Cyber attacks targeting health sector surge amid COVID-19 crisis." Verdict Medical Devices News. March 16. See https://www.medicaldevice-network.com/news/coronavirus-cybersecurity/

[2] Miller, M. and O. Beavers. 2020. "Hospitals brace for increase in cyberattacks." The Hill. April 19. See https://thehill.com/policy/cybersecurity/493410-hospitals-brace-for-increase-in-cyberattacks

[3] Kujawa, A. et al. 2019. "Cybercrime Tactics and Techniques." Malwarebytes CTNT Report. November. Report available at https://resources.malwarebytes.com/files/2019/11/191028-MWB-CTNT_2019_Healthcare_FINAL.pdf

[4] INTERPOL. 2020. "INTERPOL launches awareness campaign on COVID-19 cyberthreats. INTERPOL. May 6. See https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-launches-awareness-campaign-on-COVID-19-cyberthreats

[5] M. Uma and G. Padmavathi. 2013. "A survey on various cyber attacks and their classification." International Journal of Network Security, Vol. 15, (5), p390-396.

[6] Definition of 'malware' borrowed from the glossary published by the Computer Security Resource Center at the National Institute of Standards and Technology in USA. See https://csrc.nist.gov/glossary/term/malware

[7] Definition of 'phishing' borrowed from the glossary published by the Computer Security Resource Center at the National Institute of Standards and Technology in USA. See https://csrc.nist.gov/glossary/term/phishing

[8] Definition of 'spear phishing' borrowed from Kaspersky's Resource Center. See https://www.kaspersky.com/resource-center/definitions/spear-phishing

[9] Definition of 'ransomware' borrowed from the Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security in USA. See https://www.us-cert.gov/Ransomware

[10] Definition of 'denial of service' borrowed from the glossary published by the Computer Security Resource Center at the National Institute of Standards and Technology in USA. See https://csrc.nist.gov/glossary/term/denial_of_service

[11] Ireton, C. and J. Posetti. 2018. "Journalism, 'Fake News' and Disinformation: Handbook for Journalism Education and Training." UNESCO. See https://en.unesco.org/fightfakenews

[12] INTERPOL. 2020. "Cybercriminals targeting critical healthcare institutions with ransomware." INTERPOL. April 4. See https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware

[13] An Interpol 'Purple Notice' is an international request for member countries to seek or provide information on modus operandi, objects, devises and concealment methods used by criminals. Further details available on the INTERPOL website; See https://www.interpol.int/en/How-we-work/Notices/About-Notices

[14] INTERPOL. 2020. "Cybercriminals targeting critical healthcare institutions with ransomware." INTERPOL. April 4. See https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware

[15] Taylor, P. 2020. "COVID-19-themed cyber attacks hit healthcare bodies." Pharmaphorum. April 15. See https://pharmaphorum.com/news/covid-19-themed-cyberattacks-hit-healthcare-bodies/

[16] WHO. 2020. "WHO reports fivefold increase in cyber attacks, urges vigilance." WHO News Release. April 23. See https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

[17] Ibid.

[18] Stein, S. and J. Jacobs. 2020. "Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak." Bloomberg. March 16. See https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response

[19] Pressey, D. 2020. "C-U Public Health District's website held hostage by ransomware attack." The News-Gazette. March 11. See https://www.news-gazette.com/news/local/health-care/c-u-public-health-district-s-website-held-hostage-by/article_2daded-cd-aadb-5cb1-8740-8bd9e8800e27.html

[20] Sanger, D.E. and N. Perlroth. 2020. "U.S. to Accuse China of Trying to Hack Vaccine Data, as Virus Redirects Cyberattacks." The New York Times. May 10. See https://www.nytimes.com/2020/05/10/us/politics/coronavirus-china-cyber-hacking.html

[21] GCHQ. 2020. "Advisory: APT29 targets COVID-19 vaccine development." National Cyber Security Centre, United Kingdom GCHQ. July 16. See https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf

[22] Winder, D. 2020. "COVID-19 Vaccine Test Center Hit By Cyber Attack, Stolen Data Posted Online." Forbes. March 23. See https://www.forbes.com/sites/daveywinder/2020/03/23/covid-19-vaccine-test-center-hit-by-cyber-attack-stolen-data-posted-online/#ea8b3fd18e55

[23] Alert (AA20-126A). 2020. "APT Groups Target Healthcare and Essential Services." Cybersecurity and Infrastructure Security Agency Alerts. May 5. See https://www.us-cert.gov/ncas/alerts/AA20126A

[24] Kumaran, N. and S. Lugani. 2020. "Protecting businesses against cyber threats during COVID-19 and beyond." Google Cloud Blog. April 16. See https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond

[25] Ranger, S. 2020. "Microsoft: Beware this massive phishing campaign using malicious Excel macros to hack PCs." ZDNet. May 22. See https://www.zdnet.com/article/microsoft-beware-this-massive-phishing-campaign-using-malicious-excel-macros-to-hack-pcs/

[26] Health Sector Cybersecurity Coordination Center (HC3). 2020. "HC3: Fake Online Coronavirus Map Delivers Well-known Malware. American Hospital Association. March 10. See https://www.aha.org/guidesreports/2020-03-18-hc3-fake-online-coronavirus-map-delivers-well-known-malware-march-10-2020

[27] Cimpanu, C. and Z. Day. 2020. "There's now COVID-19 malware that will wipe your PC and rewrite your MBR." ZDNet. April 2. See https://www.zdnet.com/article/theres-now-covid-19-malware-that-will-wipe-your-pc-and-rewrite-your-mbr/

[28] United Nations Department of Global Communications. 2020. "UN tackles 'infodemic' of misinformation and cybercrime in COVID-19 crisis. United Nations. March 31. See https://www.un.org/en/un-coronavirus-communications-team/un-tackling-%E2%80%98infodemic%E2%80%99-misinformation-and-cybercrime-covid-19

[29] Spring, M. 2020. "Coronavirus: The human cost of virus misinformation." BBC News. May 27. See https://www.bbc.com/news/stories-52731624

[30] Kelion, L. 2020. "Coronavirus: France set to roll out contact-tracing app before UK." BBC News. May 28. See https://www.bbc.com/news/technology-52832279

[31] Kelion, L. 2020. "UK virus-tracing app switches to Apple-Google model. BBC News. June 18. See https://www.bbc.com/news/technology-53095336

[32] Montalbano, E. 2020. "Malicious actors could potentially harvest data over the air and use it to shake confidence in the public-health system, EFF says." Threatpost. April 29. See https://threatpost.com/google-apple-contact-tracing-system-cyberattacks/155287/

[33] United Nations Department of Global Communications. 2020. "UN tackles 'infodemic' of misinformation and cybercrime in COVID-19 crisis. United Nations. March 31. See https://www.un.org/en/un-coronavirus-communications-team/un-tackling-%E2%80%98infodemic%E2%80%99-misinformation-and-cybercrime-covid-19

[34] ANCOM. 2020. "ANCOM va aplica masurile din Decretul privind instituirea starii de urgenta pe teritoriul Romaniei." National Authority for Management and Regulation in Communications of Romania (ANCOM). March 17. See https://www.ancom.ro/ancom-va-aplica-masurile-din-decretul-privind-instituirea-starii-de-urgenta-pe-teritoriul-romaniei_6251

[35] DICT. 2020. "DICT, PNP to combat fake news on Covid-19 with Kontra Peke." Republic of the Philippines Department of Information and Communications Technology. April 5. See https://dict.gov.ph/dict-pnp-to-combat-fake-news-on-covid-19-with-kontra-peke/

[36] EC eHealth Network. 2020. "Mobile applications to support contact tracing in the EU's fight against COVID-19: Common EU Toolbox for Member States." European Commission. April 15. Version 1.0. See https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

[37] Details of the United Nations High-level Panel on Digital Cooperation are available at https://www.un.org/en/digital-cooperation-panel/

worldbank.org/digitaldevelopment

Analytical Insight

DIGITAL DEVELOPMENT

WORLD BANK GROUP
Digital Development