Пустые и необоснованные попытки разжечь напряженность: Russian Cyber-Attacks on the U.S. Healthcare System During the COVID-19 Pandemic

Пустые и необоснованные попытки разжечь напряженность: Russian Cyber-Attacks on the U.S. Healthcare System During the COVID-19 Pandemic

Crispin S. Blanchette

A Thesis in the Field of Government

for the Degree of Master of Liberal Arts in Extension Studies

Harvard University

March 2024

Abstract

Between 2019 and 2022, the United States along with the rest of the world suffered through one of history's most damaging pandemics. While the headlines focused on the human effects of the global pandemic, the U.S. healthcare system silently weathered one of the most deliberate, destructive, and persistent cyber-attacks in history. Those attacks, whether state-sponsored, state-encouraged, or state-permitted overwhelmingly originated from Russia, resulted in countless direct and indirect financial losses, disrupted care delivery across the United States, and ultimately cost American lives. The U.S. proved impotent in its reaction and response. Neither the U.S., nor Russia, curtailed this behavior during the pandemic and the conditions for continued exploitation of the U.S. healthcare system remain to this day.

Author's Biographical Sketch

Crispin S. Blanchette is a long-time healthcare technology executive, having served as the Chief Information, Chief Technology, or Chief Security Officer for six different healthcare organizations over the course of a 20+ year civilian career. His experiences covered three public and two private equity-backed healthcare companies, along with one of the world's leading academic medical centers. Prior to that, he served for more than a decade in different military roles, including infantry, special operations, and intelligence. He served as a critical infrastructure protection and cyber-security advisor during the President George W. Bush administration. Today, he works with Disabled Veterans, helping them access federal, state and community resources and runs an oral history educational foundation focused on the air war over Vietnam.

Prior to attending the Harvard Extension School, he completed a Master of Business Administration at the University of Maryland Global Campus, a Master of Science at the University of North Texas, and a Bachelor of Arts at James Madison University where he was a George C. Marshall Foundation Scholar.

Dedication

To the providers who served on the front lines during one of the nation's most challenging times, and to the technology and cyber-security professionals who worked exhaustively in the background fighting an invisible enemy.

Acknowledgments

No work of consequence is solely the product of one's own thoughts or efforts. Accordingly, it would be remiss to fail to acknowledge and appreciate the considerable efforts put forth by my academic advisors. Professor Derek S. Reveron from the U.S. Naval War College, Belfer Center, Kennedy School, and Extension School proved to be an immense help in shaping, testing, and refining many of the critical aspects of this project. His expertise in this area is unparalleled and remains an invaluable resource. Professor Michael Miner, also from the Belfer Center, Kennedy School, and Extension School provided extensive direction and support over the course of the entire program. Without either, the process and product would have been less well refined.

Being the beneficiary of an extensive network of advisors, there are far too many to acknowledge in any meaningful way. However, a limited number of advisors, colleagues, and contemporaries offered particularly valuable advice or served as a sounding board over the life of the project. Long-time healthcare Chief Security Officer's – Michael Mucha, Charles Lebo, and Joe Thomas along with cyber-industry luminaries – Bob Chaput, Mark Moore, Dan Ragsdale, and Ralph Worthington proved considerably valuable in working through different aspects of this project. To them all, I owe a tremendous debt of gratitude for their continued support.

As always, none of this came without time away from family, whose love and support cannot be appreciated enough.

Table of Contents

Chapter I.

Пустые и необоснованные попытки разжечь напряженность [1]

U.S.-Russia relations have proven tenuous in the best of times and outright adversarial at their worst. The fact that the U.S. and Russia failed to regress into a direct kinetic conflict during the Cold War represents a minor miracle. The fall of the Berlin Wall and the end of the Cold War did little to improve those relations. President Vladimir Putin picked up where his predecessors left off, running a patchwork ecosystem of loosely aligned, quasi-criminal states whose common grounds include a reticence for democracy, an affinity for corruption, and an antagonist disposition toward the United States. Even with the entire world universally impacted by the COVID-19 pandemic, U.S.-Russian relations failed to improve during this difficult period. In many respects, they worsened.

Compounding the effects of the COVID-19 pandemic and the historical pretext between the United States and Russia, the U.S. suffered one of the darkest chapters in its history. A barrage of cyberattacks directed toward the U.S. healthcare system crippled many of the nation's most critical care delivery capabilities at a time the nation needed them most. These attacks were deliberate, effective, and almost singularly directed toward America's healthcare sector. They were tactically proficient while being

[1] Translated as "Empty and unfounded attempts to inflame tensions," a phrase coined, and used regularly, by Russian Press Secretary and diplomat Dmitry Peskov.

strategically valuable. The attacks yielded millions of dollars in ransomware payments, crippled healthcare delivery systems at a time those systems were critical to the nation's COVID-19 response and cost American lives. The direct and indirect effects of these attacks prove nearly incalculable, but no less significant because of this difficult calculus.

In response, the United States chose to do little. There proved to be strikingly little mention of these attacks in the public domain. Beyond those that were required by law to acknowledge the incidents, there was little public disclosure or discourse of events. Washington failed to marshal any meaningful resources to help prevent or respond to these attacks. Seemingly acquiescent to these attacks, healthcare providers found themselves without support from the federal government while facing an onslaught of malicious behavior that overwhelmingly originated from within the borders of one of America's most virulent adversaries – Russia.

Some of the conditions that allowed the U.S. to suffer to the extent it did were self-inflicted. Following the collapse of the global capital markets in 2008, the U.S. passed the American Reinvestment and Recovery Act (ARRA), which subsidized the digitization of healthcare. With billions of dollars of federal subsidies, American healthcare providers adopted electronic health records (EHR's) at a rate and pace never previously seen.[2] This wide-spread technology adoption, however, included near-zero parameters for the adoption of commensurate security controls. Built on interconnected,

[2] The terms Electronic Health Record (EHR) and Electronic Medical Record (EMR) will be used interchangeably throughout, as the minor differences between the two terms are inconsequential to this study.

yet antiquated architectures, hospital systems unknowingly expanded their attack surface in unimaginable ways and exposed vulnerabilities that never previously existed.

Compounding this self-inflicted conundrum, malicious actors exploited this period to their benefit, launching cyberattack after cyberattack against the U.S. healthcare system. The extent to which the Russian state participated in this malicious behavior is difficult to assess. Unlike its public perception as a totalitarian state, Russia tends to operate a loosely controlled society, where lawlessness is common, and criminal behavior commonplace. Putin, as a former KGB officer, did little to curtail the unlegislated ecosystem he inherited. Provided the strategic objectives of the criminal do not conflict with the goals of the state, not only is criminal behavior tolerated, but tacitly endorsed. The proceeds from much of this criminal behavior fuel a hierarchical system of tribute paid to government leaders.

The nature of cyberspace makes attribution, or the ability to definitively ascribe malicious behavior to an individual or group, difficult. Considering the stakes involved, loose attribution presents even further pressure on analysts and investigators, as the consequences of being wrong are material. Unlike physical crimes, cybercrimes yield fewer tangible clues to the culprits behind an attack. This puts much of the burden for attribution on the select few individuals capable of assembling a vast pyramid of data to influence the level of conviction underlying an assessment. Even when an offending entity is identified with a high degree of confidence, Russia evolved its offensive cyber apparatus over time, creating space and plausible deniability between official, state-sponsored, employed entities and the offenders behind many of the pandemic attacks. The nature of these arms-length relationships further compounds America's ability to

identify specific culprits, the degree of state support they may or may not have received, and the extent to which Russia supported, endorsed, or tolerated a rogue criminal entity.

What is clear is the impact these attacks had on the U.S. healthcare system. They produced devastating outages. Providers delivered care without requisite patient data. Patients in need of care were diverted to other facilities, canceled, or delayed treatment. In some cases, patients died, a subset of American's who made the ultimate sacrifice and whose numbers are likely understated. The financial impact measured in the billions of dollars, with entities incurring costs associated with downtime, missed or canceled procedures, recovery and restoration efforts, the inability to collect cash, legal fees, fines, and finally the ransoms paid themselves.

The financial toll of these attacks may someday be fully accounted for, but the human impact will never be known. Because the death toll during this period surpassed well over one million American's, it will never be known whether those deaths were the result of the COVID-19 pandemic, the diversion of patients seeking care to other facilities, missed, or delayed treatments that caused aggressive forms of disease to progress unabated, the inability of caregivers to access records necessary to the delivery of appropriate care, or some other factor directly or indirectly tied to the healthcare systems of America being ransomed by criminals.

In response to these outrages, the federal government did nothing. Washington staffed, then eliminated, then staffed yet again national cybersecurity leadership positions. While their titles suggest both access to, and influence in, the White House, the total inefficacy of the national cybersecurity role calls into question the reality of cybersecurity as a national security priority. Much like generations of their predecessors,

national cybersecurity leadership proved wholly ineffective at raising cybersecurity to that of a national security priority and even less so ineffective at protecting our nation's critical infrastructure. While the U.S. published additional iterations of national cybersecurity strategies, implementation plans, and convened working groups and advisory bodies, nothing of consequence materialized before, during, or after COVID-19 to assuage the burdens of the private sector. Identical to the period before the pandemic, the healthcare sector remains today a high-profile target with little cover from the massive bureaucracy that sits overtop the sector, regulates most every aspect of the industry, and provides nothing of value to keep the proverbial cyber-barbarians at the gate.

For the United to States to better weather the predictable cyber-storms on the horizon, the nation needs to fully commit to a substantially more aggressive series of countermeasures. As Professor Derek Reveron explained, "in just a few short years, inexpensive computing and easy network access have broadened the scope of national security actors from states to groups to individuals."[3] The United States displays difficulty mobilizing all three: the state, groups, and individuals. Our opponents seemingly do not. During COVID-19, the U.S. remained unprepared, both for the COVID-19 pandemic and the attendant cyberattack against its healthcare system. Given the resources and resourcefulness of the United States, this remains inexcusable. America demands, and should do, better.

[3] Derek S. Reveron, ed., Cyberspace and National Security: Threat Opportunities, and Power in a Virtual World (Washington, DC: Georgetown University Press, 2012), 225.

Chapter II.

Background

"There were many warnings of the disaster coming in the financial systems and all were ignored. The present healthcare system is a medical and a financial disaster, and perhaps only the disaster itself will get bad enough to change the status quo. My fear is the government will spend billions computerizing the present chaos and will remain unaware of the fundamental changes that are so badly needed." - Larry Weed, 2009[4]

"No EMR" read a 2015 physician recruitment advertisement.[5] To think that well into the 21st century, the absence of technology would be viewed as a key differentiator in the war for talent seems almost implausible. Yet the advertisement is not only real, but a representative symptom of a bigger problem, a problem that is unique to healthcare. For decades, the healthcare industry remained hyper-resistant to technology adoption. While all industries sweepingly modernized throughout the late-20th and early-21st centuries, healthcare remained steadfast in its refusal to adopt technologies. Even after the most significant, industry-specific, technology incentive adoption program ever passed by the

[4] Lee Jacobs, MD, "Interview with Lawrence Weed, MD – The Father of the Problem Oriented Medical Record Looks Ahead," *The Permanente Journal* 13, no. 3 (Summer 2009): 84-89.
[5] Robert M. Wachter, MD, "Why Healthcare Tech is Still so Bad," *New York Times*, Sunday Opinion, March 21, 2015.

U.S. Congress, the healthcare industry remained near the bottom of McKinsey & Company's annual Industry Digitization Index.[6]

A decade prior to the shocking "No EMR" recruitment campaign, the healthcare industry continued to vehemently debate the merits of computerization. A prominent 2006, Health Affairs article argued that there existed no measurable benefit to the EMR. In fact, just the opposite was more likely true than not. Dr. Jann Sidorov argued "A considerable body of evidence suggests that widespread adoption of the EHR increases health care costs."[7] He continued "What is clear that once physician's reluctance is overcome, the EHR's business case will not necessarily be aligned with the nation's interest in lowering costs and increasing quality. As the EHR's installation and maintenance expenses pass to the consumer through increased billings – absent any economic return on efficiency or quality – costs are likely to be accelerated."[8] Critics of EHR adoption challenged every aspect of the EHR adoption narrative – cost, quality, access, and convenience. No element of the healthcare computerization business case remained unopposed. Seemingly all of American society welcomed technological advancement, automation, efficiency, and computer-aided intelligence, yet the healthcare industry remained staunchly unconvinced. Imbued with the principles of autonomy and a deep concern for patient safety and welfare, broad healthcare computerization remained low well into the first decade of the 21st century.

---

[6] McKinsey & Company, "Digital is Reshaping U.S. Health Insurance – Winners are Moving Fast," January 8, 2019, https://www.mckinsey.com/industries/healthcare/our-insights/digital-is-reshaping-us-health-insurance-winners-are-moving-fast.
[7] Jann Sidorov, MD, "IT Ain't Necessarily So: The Electronic Health Record and the Unlikely Prospect of Reducing Health Care Costs." *Health Affairs* 25, no. 4 (2006): 1079.
[8] Ibid, 1083.

Many of these dynamics changed when the U.S. economy crashed in 2008. With the crashing of the market came the passage of H.R.1, the American Reinvestment and Recovery Act (ARRA) on February 17, 2009. The Congressional Research Service (CRS) described this ambitious bill as "one of the most significant legislative responses ever." The CRS continued, "ARRA is a relatively lengthy and complex act, amounting to just over 400 pages…. ARRA provides almost $800 billion through extensive discretionary spending, mandatory spending, and revenue provisions that the Administration estimates will save or create some 3.5 million jobs."[9] Unsurprisingly, America's response to the challenges in the public markets, the housing markets, and the global markets was a massive infusion of cash into critical elements of the U.S. economy.

Embedded within ARRA were more than $35B in healthcare technology investments designed to put an end to the debate around healthcare technology and mandate adoption through a series of both incentives and penalties.[10] Critics of this approach immediately emerged arguing against many aspects of ARRA. One prominent op-ed argued "The assumption underlying the proposed investment in health IT is that more and better clinical information will improve care and save money. But the benefits of health IT have been greatly exaggerated. Large, randomized, controlled studies – the 'gold standard' of evidence – in this country and Britain have found that electronic records with computerized decision support did not result in a single improvement in any

[9] Congressional Research Service, "American Reinvestment Act of 2009 (P.L. 111-5): Summary and Legislative History," Washington, DC: https://crsreports.congress.gov/R40537.
[10] John Tune, Lamar Alexander, Pat Roberts, Richard Burr, and Mike Enzi, "Where is HITECH's $35B Investment Going?" *Health Affairs*, March 4, 2015, https://doi.org/10.1377/forefront.20150304.045199.

measure of quality of care for patients with chronic conditions."[11] The Washington Post Op-Ed concluded that "health IT has not been proven to save money."[12]

Despite these compelling arguments, government leaders on both sides of the aisle remained convinced that healthcare IT saved money, improved efficiencies in the healthcare ecosystem, and ultimately saved lives. The highest authorities in the land put the healthcare industry on notice and advised the industry they were expected to drive technology adoption or suffer the consequences of failing to do so. Healthcare faced the proverbial carrot or stick. Along with substantial financial incentives to adopt certified electronic health records came similarly substantial penalties for failing to meet adoption timelines. For an industry that is heavily reliant on federal funding to remain solvent, avenues to work over, under, or around the Congressional mandate were exhausted.

While the White House and Congress laid down the gauntlet, there remained a steep technology adoption curve ahead. It is one thing to allocate money against a problem. It is entirely another to achieve the goals and objectives of that appropriation. At the time that ARRA became law, less than half of the healthcare industry employed an even basic electronic medical record.[13] After pioneering much of the worldwide research, thought leadership, and EMR advocacy - including the development of the very systems themselves - in 2008 the U.S. remained a full generation behind its western peers in EMR adoption. To put this in context, there existed near universal adoption of EMR's

[11] Soumerai, Stephen B. and Majumdar, Sumit,R. "A Bad $50 Billion Bet." *Washington Post*, Opinion Page, March 17, 2009.
[12] Soumerai, Ibid.
[13] Henry, JaWanna, et al, Adoption of the Electronic Health Record Systems Among U.S. Non-Federal Acute Care Hospitals, 2008-2015. ONC Data Brief 35, May 2016, https://dashboard.healthit.gov/evaluations/data-briefs/non-federal-acute-care-hospital-ehr-adoption-2008-2015.php.

in comparable healthcare systems around the globe at the same time, including the Netherlands (99%), Norway (97%), New Zealand (97%), the United Kingdom (96%), and Australia (95%). The United States (46%), and somewhat surprisingly Canada (37%), remained inexplicably out of the EHR adoption universe at the time that ARRA became law.[14]

It was not until substantial EHR incentive payments, and the corresponding penalties, embedded within ARRA that the healthcare industry began to digitize in a meaningful way. Between 2008 and 2018, EHR adoption nearly doubled, with 86% of the industry reporting usage of an electronic health record.[15] Physician EHR adoption surpassed 90%. While not yet achieving universal adoption seen in other countries, the U.S. nearly doubled EMR adoption in less than a decade, an impressive feat, especially within the context of the preceding decades.

Despite this meaningful progress, cyber-security analysts with cross-sector visibility raised red flags. While pre-ARRA healthcare was oft derided for its lack of technology adoption and poor technical sophistication, post-ARRA healthcare possessed all the warning signs of an industry on the brink of technological disaster. Cybersecurity firm SwivelSecure published a 2018 opinion piece that outlined "9 reasons why healthcare is the biggest target for cyberattacks."[16] Much of this article could have been published about any industry – outdated technology, the significance and monetary value

[14] Schoen, Cath, Osborn, Robin, et al, "A Survey of Primary Care Doctors in Ten Countries Shows Signs of Progress in Use of Health Information Technology, Less in Other Areas," *Health Affairs* 31, no. 12 (December 2012), https://doi.org/10.1377/hlthaff.2012.0884.
[15] Julia Adler-Milstein, A Jay Holmgren, Peter Kralovec, Chantal Worzala, Talisha Searcy, Vaishali Patel, "Electronic Health Record Adoption in US hospitals: The emergence of a digital "advanced use" divide," *Journal of the American Medical Informatics Association* 24, Issue 6 (November 2017): 1142–1148, https://doi.org/10.1093/jamia/ocx080.
[16] https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/

of the underlying data, poor user awareness, education, and training programs, all could have been attributed near-universally to any industry. Yet, there were elements of this assessment that proved uniquely healthcare and prescient in their prediction. SwivelSecure underscored the reticence of healthcare practitioners to change their tried-and-true practices, the necessity of open access and the relatively free flowing nature of data amongst large communities of providers, and the explosion in vulnerable medical devices that became ubiquitous because of massive government incentives that drove technology adoption.

With rapid digitization came risks, risks the healthcare industry remained woefully unprepared to address. Much like a seven-foot-tall child, healthcare industry computerization came with substantial growing pains. Journalist and editor Jessica Davis characterized this transition saying, "the unintended consequence of this digital explosion was a new and significant risk to business and clinical operations resulting from outages in EHR and other new automated systems."[17] Hospitals and health systems unknowingly created reliabilities on untested systems, and inherited vulnerabilities and capability gaps where few previously existed. Because of the completeness of these new electronic health records – systems that spanned everything from scheduling, communications, workflow, clinical records, images, medications and medication administration, laboratory results, and billing – over reliance on these enterprise-wide systems created substantial vulnerabilities never previously imagined.

[17] Jessica Davis, "Health Care a Culture of 'Yes': How EHR modernization raises cybersecurity challenges." *SC Magazine*, August 23, 2021, https://www.scmagazine.com/feature/risk-management/health-care-a-culture-of-yes-how-ehr-modernization-raises-cybersecurity-challenges.

And while post-ARRA digitization proved new for the healthcare industry, the platforms they adopted were anything but modern. Industry leaders Epic and Cerner were both founded in 1979 and layered decades upon decades of development on top of antiquated underlying architectures. Professor Rose Bernard summarized the situation as "hospitals and healthcare systems often employed legacy IT systems, which proved vulnerable to attack."[18] She continued that "the intricacy of interactions between the variety of systems and the people using them leaves health systems open to a wide range of cyber-attacks."[19] Hyper-connected, antiquated systems, operated by individuals with limited experience in computer security foretold a rocky road ahead.

In the case of the healthcare provider organization, they possessed none of the tools necessary to remedy these vulnerabilities. Few information technology experts, and fewer notable cybersecurity experts worked in the field of healthcare for many of the reasons previously discussed around technology obsolescence. Experts from outside the field of healthcare proved a difficult fit within the liberal confines of healthcare institutions. Unsurprisingly, the controls that worked in banking, defense, or telecommunications proved impractical in a field where human lives depended on the immediacy and completeness of patient-specific data. The speed with which the cybersecurity threat emerged, and the poor talent base employed within the industry, proved to be a monumental challenge. It is reasonable to conclude that in an industry that

[18] Rose Bernard, Gemma Bowsher & Richard Sullivan, Cyber Security and the Unexplored Threat to Global Health: A call for global norms, *Global Security: Health, Science and Policy* 5, no.1 (2020): 134-141, https://doi.org/10.1080/23779497.2020.1865182.
[19] Ibid.

advertises "No EMR," few of the best and brightest minds in the field of security sought employment.

Compounding the talent acquisition issue was the proprietary nature of these systems – often hosted on a proprietary and inaccessible cloud – ensured that even the most responsible healthcare providers could not make necessary security changes to the software or the infrastructures upon which that software relied. Until recently, both Epic and Cerner ran proprietary data centers, far removed from their customers grasp, and whose only tangible security countermeasures existed in a series of contractual service level agreements and penalties for failure or breach. Even the ability to audit, inspect, or assess the controls of the largest EMR providers were precluded, diluting even the best and most well-intentioned risk management efforts.

To make matters worse, consider the size and scope of the enterprise. The healthcare sector represents nearly 20% of the gross domestic product and employs slightly more than one in five workers in America.[20] Hospitals and health systems tend to be large, and in many cases are the largest employer in many metropolitan areas. "The potential attack surface of any hospital or medical facility is vast, given the complexity of systems within it, the breadth of people employed, and the use of third- party suppliers and software."[21] Being the largest operator of the critical infrastructure sectors, the largest employer of the critical infrastructure sectors, and the sector scaling its digital

[20] Aytan Dahukey, Kenneth Yood, and Samuel O'Brien, "Venture Capital and Private Equity Investors Take Note: Primary Care May Become the Next Behavioral Health," August 5, 2020, https://www.lexology.com/library/detail.aspx?g=ef6ca53f-d115-4a57-a5e6-ace9baf7c2af

[21] Rose Bernard, Gemma Bowsher & Richard Sullivan, "Cyber Security and the Unexplored Threat to Global Health: A call for global norms," *Global Security: Health, Science and Policy* 5, no. 1 (2020): 134-141, https://doi.org/10.1080/23779497.2020.1865182.

footprint rapidly to catch up with other sectors, the healthcare industry emerged post-ARRA ripe for exploitation.

Beyond a lack of technological sophistication, poor vendor security, and a lack of embedded security expertise, the consequences of outages in healthcare can be severe. "When computer systems go offline, everyone feels the stress of conducting business and delivering care without access to all the information they need. Downtimes are especially dangerous for patients."[22] Stress to caregivers can create an unsafe care delivery environment, and an unsafe environment may present dire consequences for patients under the care of those struggling with system outages. The inability to marry up imaging data, pharmacy data, medical history data, patient self-reported data, and clinical orders has the potential to create a deadly care delivery environment for patients, and a highly stressful environment for care providers.

Finally, there are other considerations beyond the scale of the footprint, the over-reliance on poorly designed electronic systems, and the consequences of failure. Hospitals and health systems operate in a highly regulated environment, one that demands transparency in nearly every aspect of its business. There are security and privacy considerations, quality and patient safety considerations, legal considerations, and innumerable other elements of provider performance that are publicly reportable and made widely available. This regulatory vulnerability creates undo exposure for healthcare providers. "The criticality of hospital services, combined with the potential for reputational and legal damage, means that hospitals are perceived by threat actors as

[22] Drexel Deford, "Sustainable Digital Health Demands Cyber Security Transformation," *National Library of Medicine PubMed* 38, no. 3 (April 1, 2022): 31-38, https://doi.org/10.1097/HAP.0000000000000137.

more likely to meet ransom demands, a view borne out by discussions on criminal forums."[23]

The industry made tremendous strides post-ARRA, driving EMR adoption, providing intelligence to providers in novel and efficient ways, and helping to reduce the pervasiveness – and confines – of paper across the industry. Limitations remained, and the industry continued to balance the attendant benefits and risks associated with technology adoption and ultimately emerge at a better place. Growing pains remained and the industry continued to battle with usability concerns, but fundamentally the industry faced skilled security labor challenges coupled with large footprints of antiquated systems. By 2019, the healthcare sector transitioned from one that was woefully uninteresting to one that was highly digitized, scaled extensively, and immature in its understanding of information systems risk management practices. At a time when the industry needed its systems the most, at the height of the global pandemic, malicious actors from across the seas targeted these vulnerable systems and set to exploit many of the vulnerabilities that failed to exist in the era of "No EMR."

[23] Rose Bernard, Gemma Bowsher & Richard Sullivan, Cyber Security and the Unexplored Threat to Global Health: A call for global norms, *Global Security: Health, Science and Policy* 5, no. 1 (2020): 134-141, https://doi.org/10.1080/23779497.2020.1865182.

Chapter III.

Threat Picture

Arguing that Russia exploited U.S. exposure to, and focus on, the COVID-19 pandemic makes several implications that are overly broad and highly generalized. First, it would suggest that Russia, or more specifically the Russian state, is a hegemonic actor that operates in a unified fashion with singular purpose. Unlike China, there exists substantial room in Russian society for quasi-state supported actors, relatively independent entrepreneurs, and even criminal organizations to operate with near autonomy. Second, it suggests that the U.S. served as the target, when it is more likely than not that financial opportunity proved to be the target for most actors, and it was America's affluence that provided an unfortunate proxy to Russian focus on the U.S. Third, this narrow argument eliminates the possibility, or even probability, that other states acted in a similar way, toward a similar end, during overlapping periods of time. There is little question that there was a substantial uptick in targeted cyberattacks on the U.S. during this period, the disproportionate share of those attacks impacted the U.S. healthcare industry, and most assessments tie those events back to Russia. Despite the preponderance of evidence that points toward the Russian origin for these healthcare-directed cyberattacks, this does not preclude the possibility that more than one malicious actor exists in the interconnected cyberworld, and those actors may have acted in strikingly similar ways.

When it comes to an effective centralized administrative apparatus, China, Russia is not. President Vladimir Putin inherited a country reeling from the fall of the Iron Curtain and a society that reveled in lawlessness. While Putin put in place some framework to corral the most egregious lawless activity, few of the controls put in place by the central government curtailed all lawless behavior, in particular when that lawless behavior supported the interests of the state.

By creating an Oligarchy, or at least enabling an Oligarchy, Putin effectively endorsed an entrepreneurial environment that paid tribute to, and was highly dependent upon, the central state. These actors, while supported by, aligned with, or at the very least not in conflict with the Russian state, tended to be motivated more by the opportunistic nature of financial cybercrime than the benefits those activities accrue for the state. Yet, as is the case with many paradoxical relationships, two things can be true at the same time. Putin can simultaneously exhibit an air of totalitarianism while allowing for a wildly independent, if not outright criminal, subsegment of society to operate with impunity; especially when their aims might be in alignment and their financial proceeds shared amongst the ruling class.

There exist innumerable cases where the financial interests of Russian cyber-criminals and the national strategic objectives of the Russian state are in clear alignment, especially when targeting well capitalized components of the U.S. critical infrastructure. This is even more so true during an unprecedented pandemic influenza outbreak where reliable information portability was slow, government leadership questionable, and response to a national emergency of immense significance poorly orchestrated and

executed. As Professor Reveron articulated, "Unfortunately, the federal government's feeble response to COVID-19 mirrors its response to the cybersecurity threats created by ransomware, intellectual property theft, and identity theft."[24] It is not only possible, but likely, that both the Russian state and Russian cybercriminals resident in the state recognized America's sloppy response to COVID-19 as an opportunity to further exploit an inherently vulnerable and increasingly overtaxed healthcare system during a period of crisis.

The Threat Universe

Before a more detailed analysis on attribution, or who the likely culprit or culprits may have been during the COVID-19 period can be articulated, it is important to establish some fundamentals about the types of threats pervasive during the COVID-19 pandemic. It is safe to acknowledge that there was no shortage of every type of malicious event during this period. Nation-states, cybercriminals, and entrepreneurial individuals took no time off during COVID. In fact, just the opposite proved true, as the data indicated an uptick in malicious cyberactivity across the globe during the pandemic.

When one sees headlines like "The COVID-19 pandemic drastically escalated cyber issues" and "Daily cybercrime complaints increased by 300 – 400 percent" it is important to understand the details underlying these headlines.[25] While undeniable that

[24] Derek S. Reveron and John E. Savage, "Cybersecurity Convergence: Digital human and national security," *Foreign Policy Research Institute (*August 2020): 560, https://doi.org/10.1016/j.orbis.2020.08.005.
[25] Mark Fichtenkamm, Gerald F. Burch, and Jordan Burch, "Cybersecurity in a COVID-19 World: Insights on how decisions are made," *ISACA Journal* 2 (2022): 1.

cybersecurity activity reached an all-time peak during COVID, not all malicious cyberactivity is created equal. Cyber events can run a spectrum from innocuous and commonplace to complex, human-dependent activities like computing to the opposite end of the spectrum where attacks are deliberate, destructive, and intended to incapacitate specific targets.

During COVID, well-intentioned operators were just as likely to fail to conduct backups, lose unencrypted physical media, or forget to patch systems on regular cycles. To err is human, and the complexities of modern computing result quite routinely in human error. However, a recent IEEE study assessing cyberattacks during COVID-19 identified "ransomware, malware, spam emails, malicious domains and (Distributed Denial of Service) DDoS" as the most pervasive and common threats during the assessed period."[26] Put differently, the data suggests that there appeared to be no more or less security issues attributed to the normal course of business, yet the frequency of ransomware and other forms of malware skyrocketed.

Distributed denial of service attacks are a common component to the modern malicious actor's toolbox. DDoS attacks seek to take a target offline by flooding their systems, especially their pubic facing systems, with connection requests that eventually cause the system to fail. Malicious domains are an attempt to establish a web presence that mimic a legitimate entity, often re-directing traffic in an effort to compromise information or propagate misinformation. Spam emails, almost as old as email itself, are

---

[26] Navid Ali Khan, Sarfraz Nawaw Brohi, and Noor Zaman, "Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic," *TechRxiv* (2020), https://doi.org/10.36227/techrxiv.12278792.v1.

a similar tactic using malicious email to appear legitimate when it is not. These three capabilities do not represent much in the way of sophistication, as they are common, inexpensive, and an everyday technique employed by even the most basic of malicious actors. Because of their pervasiveness, lack of sophistication, and ease of deployment, they are the garden variety tools, techniques, and tactics used by individuals and organizations worldwide.

Ransomware and malware, the former being a subset of the latter, represent an entirely different caste of offender. Not only are they comparably difficult to manufacture, but they also offer substantial promise for the purposes of determining critical elements about a cyber-incident – source, target, means, and to some extent the architect behind the event. Malware, much like the enabler of any crime, leaves behind clues that are indicative of many aspects of that crime. And much like physical crimes, there is an entire body of experts trained in cyber forensics who can identify methods and culprits engaged in malware development and propagation. Because of the maturity of this profession, along with collaboration between forensic experts, the intelligence community and the law enforcement community, analysts today can refine their understanding of cyber-events in ways approaching physical forensics.

While DDoS attacks, spam emails, and malicious domains are commonplace and oft-used methods employed by reasonably unsophisticated entities, malware and ransomware take some degree of skill to develop, deploy, and operate. It was not until late-2022 or early 2023 that organizations offering "ransomware-as-a-service" became well known and broadly accessible. Prior to the professionalization and corporatization

of ransomware, it took skill and sophistication to successfully operate malware or ransomware in a replicable fashion. Simultaneously attacking multitudes of entities, operating as a large, capital intensive, financially profitable enterprise is not representative of a fly by night operation. In many cases, these types of attacks suggest the perpetrators look more like big business – entities with big payrolls, human capital and talent acquisition challenges, large capital infrastructures, and steady streams of revenue to support a going concern. If a malware or ransomware actor is not a commercial enterprise, then they are more likely than not a state-run or state-supported entity, reliant on the state to address the capital and human resource needs of running a complex, global, computing enterprise at scale.

Narrowing the Threat Universe: Malware and Ransomware

To better understand the threat picture, it is helpful to dissect the most pervasive form of malware during COVID-19, ransomware. The Institute for Security + Technology described ransomware as "a sub-category of malware, a class of software designed to cause harm to a computer or computer network."[27] The U.S. Cybersecurity and Infrastructure Security Agency (CISA) defines ransomware as "an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated

[27] Institute for Security + Technology, "Combatting Ransomware: A comprehensive framework for action, key recommendations from the Ransomware Task Force," https://securityandtechnology.org/wp-content/uploads/2021/06/IST-Ransomware-Task-Force-Report.pdf.

data or authentication information if the ransom is not paid."[28] Until recently, ransomware was largely the domain of relatively sophisticated entities. To develop a malware payload, to deploy that payload with a high probability of penetrating the target, and then to conduct a corresponding criminal financial transaction is no small task.

To be successful in this endeavor, an organization is required to be competent in software development, human factors or social engineering, target analysis and exploitation, and financial crimes. They must also be cognizant that their crimes will likely be exposed to the highest levels of government and industry, and likely require substantial state-level support to engage in a continuing criminal enterprise. There are corresponding costs to acquire the talent and infrastructure to support this endeavor, and in many cases, do so in a manner that eludes international law enforcement bodies. If an organization were to do so within the confines of a country like Russia or China, there are further legal and political hurdles to navigate, as entrepreneurial and rogue criminal enterprises in either country would likely garner sufficient attention to meet an unfortunate end. This sort of political connectivity and influence is neither commonplace, nor inexpensive, to acquire and support in perpetuity. While perhaps unnecessary for an oligarch to engage in, or provide patronage to such an activity, the capital requirements, and operating complexities of such an enterprise demand an exceptionally high degree of business acumen, political access and influence, and operating sophistication.

[28] Cybersecurity and Infrastructure Security Agency, Ransomware 101, https://www.cisa.gov/stopransomware/ransomware-101.

Despite these challenges, ransomware remains big business, and the actors involved continue to get better at their trade. Recently, security firm Sophos reported that in "76% of ransomware attacks against surveyed organizations, adversaries succeeded in encrypting data. This is the highest rate of data encryption from ransomware since Sophos started issuing the report in 2020."[29] Considering the financial, infrastructural, human capital, political, and legal challenges this type of business represents, it is difficult to imagine a more complex business to operate. If not a state-run or state-sponsored entity, the ransomware syndicates are highly capable enterprises able to perpetually navigate the difficult and dangerous waters that bound their business. Clearly the costs, risks, and barriers to entry inherent in running a ransomware enterprise are substantially outweighed by the benefits in so doing. Unfortunately for the U.S. healthcare system, this remained particularly true during the COVID-19 pandemic.

Healthcare industry analyst Joel Witts further broke down the trends during COVID-19. He wrote, "Data breaches in healthcare climbed for the past five years, rising a massive 42% in 2020 when the pandemic hit. Of the total amount of ransomware attacks reported in 2020, 60% targeted the healthcare sector."[30] He continued, "in September last year *alone* researchers found 68 healthcare ransomware attacks had taken place around the world. 60% of healthcare ransomware attacks took place in the United States, with medical clinics being the most frequently attacked."[31] His analysis suggests

[29] Sophos, "Data Encryption from Ransomware Reaches Highest Level in Four Years Sophos' Annual State of Ransomware Report Finds," May 10, 2023, https://www.sophos.com/en-us/press/press-releases/2023/05/data-encryption-ransomware-reaches-highest-level-in-four-years.
[30] Joel Witts, "Healthcare Cyber Attack Statistics 2022: 25 Alarming data breaches you should know," *Expert Insights,* March 28, 2023, https://expertinsights.com/insights/healthcare-cyber-attack-statistics.
[31] Ibid.

that both method (ransomware), and target (healthcare) are quantifiable, country- and industry-specific.

A South African research team who independently assessed behavior during the pandemic period supported Witt's depiction. They concluded, "Cybercriminal syndicates are well-versed with global trends, have up-to-date information and know very well that everyone is focusing on the COVID-19 pandemic; therefore, with advanced intelligence, these criminals are attacking information systems designed to help fight the pandemic. These well-orchestrated attacks on information systems demonstrate the level of intelligence inherent in the minds of cybercriminals, prompting the global village, specifically cybersecurity and information systems experts, to be worried about the scourge."[32] The U.S. Cybersecurity & Infrastructure Security Agency confirmed the same. In December 2020, CISA Interim Director Brandon Wales stated that "due to the global pandemic, the risk landscape shifted dramatically over the last eleven months. In March (2020), CISA launched an effort to provide enhanced cybersecurity support to high- risk entities in the healthcare sector. When the Administration established Operation Warp Speed, CISA joined the interagency effort to offer cybersecurity services."[33]

Regardless of the dataset supporting the detailed assessment of malicious behavior during the COVID-19 pandemic, there is an overwhelming trove of data to

[32] Joel Chigada and Rujeko Madzinga, "Cyberattacks and Threats During COVID-19: A systematic literature review," *South African Journal of Information Management* 23, no.1 (19 FEB 2021), https://doi.org/10.4102/sajim.v23i1.1277.
[33] Brandon Wales, "State and Local Cybersecurity: Defending our communities from cyber threats amid COVID-19," U.S. Senate Committee on Homeland Security and Government Affairs, Subcommittee on Federal Spending Oversight and Emergency Management, December 2, 2020.

demonstrate that cyberattacks during this period came in the form of reasonably sophisticated malware – especially ransomware – and the target of that malware was the healthcare industry who found itself battling an unprecedented series of critical priorities. Healthcare systems worldwide, and more often in the U.S., found themselves at the mercy of cybercriminals demanding financial remuneration or threating distribution or destruction of an entities systems and data.

This narrative becomes more complex when one considers that the act of encrypting files, demanding payment, and fulfilling financial terms is not the end of the story. As the Institute for Security + Technology accurately described, "Ransomware is not just financial extortion; it is a crime that transcends business, government, academic, and geographic boundaries. It has disproportionately impacted the healthcare industry during the COVID pandemic, and has shut down schools, hospitals, police stations, city governments, and U.S. military facilities. It is also a crime that funnels both private funds and tax dollars toward global criminal organizations. The proceeds stolen from victims may be financing illicit activities ranging from human trafficking to the development and proliferation of weapons of mass destruction."[34]

Healthcare entities not only struggled with the prospects of losing data, diminished operational capacity, and the interdiction of care delivery to patients. These same healthcare entities were confronted with the prospect that their ransom payments potentially funded human-trafficking, narco-trafficking, terrorism, or weapons proliferation. Healthcare operators, struggling to survive COVID confronted

[34] Institute for Security + Technology, "Combatting Ransomware: A comprehensive framework for action, key recommendations from the Ransomware Task Force," https://securityandtechnology.org/wp-content/uploads/2021/06/IST-Ransomware-Task-Force-Report.pdf.

reputational, legal, and other challenges tied to the illicit nature of these payments and the universe of unconscionable activity their ransomware funding may support.

To say the healthcare industry struggled during the COVID-19 pandemic is an immense understatement. Compounding challenges with every aspect of care delivery, including supply chain, personnel, unprecedented loss of life, and the virus itself, they routinely awoke each day to the prospect of more bad news. Focused, sophisticated, and potentially crippling cyberattacks brought many institutions during this period to a near stand-still. Absent the electronic health records upon which hospitals became reliant, hospitals found themselves paralyzed with a diminished ability to effectively deliver care to a population in extraordinary need. The culprits behind such a sick and twisted plot could not have had anything but the worst of intentions for Americans and could not have been more deliberate in their methods to target a segment of society fundamental to basic human survival at one of the nation's most critical junctures.

Chapter IV.

Attribution

A fundamental challenge with attribution is in part the limitations inherent in cyber forensics and in part the complexities in understanding sophisticated global computing operations. Unlike physical crimes, cybercrimes lack many of the generally accepted forensic elements one might investigate as part of a physical criminal investigation. There are no eyewitness accounts, no smoking gun, no fingerprints, and no legal precedence of consequence to guide what constitutes useful forensic data. A 2015 *Journal of Strategic Studies* article explained, "Attribution is fundamental. Human lives and the security of the state may depend on ascribing agency to an agent. In the context of computer network intrusions, attribution is commonly seen as one of the most intractable technical problems, as either solvable or not solvable, and as dependent mainly on the available forensic evidence."[35] In the case of sophisticated global malware operations, attribution becomes not only technically complex, but compounded by the political realities, and in some cases the priorities or narratives of the parties involved.

The nature of global politics, or politics in general, creates an environment where attribution and political narratives become inextricably intertwined. King's College scholars Thomas Rid and Ben Buchanan posed the question, "Is this a productive understanding of attribution?"[36] They argued that often "attribution is what states make

---

[35] Thomas Rid & Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, nos. 1-2 (2015): 4-37, https://doi.org/10.1080/01402390.2014.977382.

[36] Rid and Buchanan, Ibid.

of it."[37] This political reality compounds the already difficult task of understanding who was the likely culprit behind the sophisticated attacks on the healthcare sector during COVID-19, and to what degree of confidence we ascribe to such an assessment given the complexities of geopolitical influence. As discussed previously, these are no mere fly by night outfits. These organizations are scaled, sophisticated, well-capitalized enterprises with substantial political influence and global reach. To gain a better understanding of the universe of possible culprits, it is important to narrow that universe to a more inspectable and finite list of entities that possess the motive and means to accomplish such a complex task – at scale – and succeed in significantly disrupting care delivery during the critical COVID-19 pandemic.

Narrowing the Aperture: The Usual Suspects

Without tackling the extent of national support for a particular activity now, there are a limited number of nation-state actors who possess the human, technical, and financial resources to pull off an event comparable to what the U.S. experienced during COVID-19. Clearly the U.S. and its allies across the Far East, Europe, and the "Five-Eyes" have the capacity to engage in global cyberwarfare. It is also possible that large criminal entities operating within these countries could engage in sophisticated ransomware activities, albeit unlikely. Given the degree of inspection and introspection the healthcare industry experienced in the allied nations during this period, attacks on that

[37] Rid and Buchanan, Ibid.

same infrastructure that originated from home would likely have been dealt with rather aggressively and unceremoniously.

There exist other entities around the world that have historically been party to malicious activity, in particular entities in eastern Europe, Africa, south Asia, and South America. They represent an unlikely culprit for different reasons. The attack profile and signatures originating from these regions tend to rely on social or human factors engineering, they tend to rely on the large-scale deployment of inexpensive and uneducated human labor and tend to be highly unsuccessful in their net effect on any particular target. They operate on a small scale, tend to be highly portable in their operating epicenter, and generally easy to stand up and stand down as the situation warrants. Their level of technical sophistication is not exceptional, often relying on social engineering, coupled with a reliance on less complex technologies. Spam, denial of service, and socially engineered email and phone call campaigns tend to be the primary signature for these geographies. Criminal and situationally effective, these efforts are decidedly unlike the sophisticated ransomware campaigns launched during COVID-19.

The U.S. intelligence community publishes an annual threat assessment, and with great regularity find that China, Russia, Iran, and North Korea continue to pose the greatest threat to the U.S., including information gathering and espionage, but also in the form of malicious cyber-activity.[38] These nation-states possess the means to develop,

[38] Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 6, 2023, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

deploy and operate a sophisticated malicious cyber operation against the U.S., and they possess the motivation to do so. However, not all maligned actors are the same, so it is unlikely that all four of these entities were equally engaged in this sort of malicious behavior, and even more so unlikely to have collaborated in so doing.

North Korea and Iran are the most easily discounted as the primary culprits behind these attacks. In both cases, the entities have substantial hurdles to address to engage in global financial commerce. Sanctions against both North Korea and Iran make it nearly impossible for an American institution to pay organizations associated with either country. Healthcare organizations worldwide remain exceptionally traditional in their financial operations, and few are conversant in the workarounds to these sanctions like cryptocurrency. North Korean and Iranian inabilities to use the traditional global financial markets makes participation in this sort of activity extremely complex, perhaps even more complex than the underlying technical challenges. If one is unable to profit from a complex, global, criminal enterprise, of what use is the enterprise?

In addition, both North Korea and Iran have nuclear development ambitions that remain tenuously plausible, something that could be severely impacted by the introduction of another Stuxnet-like event. Stuxnet represented a massive threat to Iranian nuclear development, setting the program back many years, and had a crippling effect on infrastructure critical to their nuclear development efforts. On several occasions, the U.S. demonstrated not only an ability, but an aptitude to deploy offensive cyber weapons in a highly directed and effective manner. It is likely that had attribution for the cyberattacks on the U.S. healthcare system during COVID-19 been even loosely

attributed to either North Korea or Iran, the U.S. response would have been highly disruptive to the nuclear ambitions of both countries.

Finally, the U.S. has very strong, highly capable, and motivated allies in South Korea and Israel that do an admirable job keeping North Korea and Iran busy enough with the traditional back and forth of nation-state cyberwarfare to find time and resources to focus on the U.S. healthcare system. While these two entities possess both means and motivation to harm the U.S., it is improbable that they participated in this activity in any meaningful manner during COVID-19. Given the questionable financial upside, the risks and consequences of so doing, and their focus on keeping South Korea and Israel at bay while pursuing their nuclear ambitions, it is unlikely that attacks of against the U.S. healthcare ecosystem would rise to the top of the priority list for either country.

China

Conversely, China possesses none of these limitations. They are a major leader in the global financial markets, possess a deep and rich talent pool of cyber experts, and have the motive and means to exploit any sector of the U.S. critical infrastructure. They fear none of their regional co-habitants. While bordered by adversaries, or potential adversaries, they possess limited strategic concern for the threats any of them pose individually, or collectively. They are winning the regional arms race, expanding their sphere of influence aggressively, and disrupting the post-World War II balance of power. They are simultaneously repositioning themselves as the regional banking hub and key influencer in hemispheric banking leadership. As Harvard Professor Graham Allison said, “China is also absorbing the nations of Southeast Asia into its economic orbit and

pulling Japan and Australia in as well. It has so far succeeded without a fight. But if fight it must, Xi intends to win"[39]

China's military modernization program extends well beyond the traditional battlefield. According to the ODNI 2023 Annual Threat Assessment "China probably currently represents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private-sector networks. China's cyber pursuits and its industry's export of related technologies increase the threats of aggressive cyber operations against the U.S. homeland. . . China almost certainly is capable of launching cyber-attacks that could disrupt critical infrastructure services within the United States."[40] The Chinese cyberthreat is credible, contemporary, and supported by a history of successful exploits against different components of the U.S. critical infrastructure.

China, however, possesses different motivations and represents a different threat profile than other actors. The Deputy Assistant Attorney General described this distinction in 2020 Senate testimony. "China, in particular, has for years sponsored computer intrusions to steal trade secrets and other confidential business information from American companies (among others) for the apparent benefit of its own industries, to give them a competitive advantage or to advance its military."[41] As far back as the early 2000's, cyber events that impacted U.S. military, intelligence, research, academic, and advanced technology efforts have regularly been attributed to Beijing. State

[39] Graham Allison, *Destined for War: Can America and China Escape Thucydides's Trap?* (Boston: Mariner Books, 2017), 128.
[40] CISA, "China Threat Overview and Advisories," https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/china.
[41] Adam S. Hickey, "Dangerous Partners: Big Tech and Beijing," U.S. Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism," March 4, 2020.

advancement and strategic prioritization of cyber-espionage, malicious computing, and other forms of cyberwarfare tends to shape the volume, velocity, and target of activities originating from China. They also tend to be generally quiet, and to a large extent, not financially motivated – at least not directly – in the execution of malicious cyberactivity originating from within the PRC.

Another aspect unique to China is the relatively regimented nature of the state. While some capacity for entrepreneurialism exists within China, their tolerance for lawlessness looks nothing like Russia. There may exist small pockets of state-aligned independent actors operating within China, but it is almost certain that China's control of all network traffic in to and out of the People's Republic would suggest that this activity is at the very least known, if not monitored and managed. A 2014 article assessing the evolution of Chinese malicious behavior suggested that even the small rogue elements of society had been professionalized by the state. The article explained, "Beijing hotly denies accusations of official involvement in massive cyberattacks against foreign targets, insinuating such activity is the work of rogues. But at least one element cited by Internet experts points to professional cyber spies: China's hackers take the weekend off."[42]

If the argument about the professionalization of Chinese malicious cyber behavior is accurate – it is professional, managed, targeted, sophisticated, and operates to a large extent to advance the interests of the state – that leaves rogues

[42] Christopher Bodeen, "Sign That Chinese Hackers Have Become Professional: They Take Weekends Off," *Huffington Post*, February 26, 2013, https://web.archive.org/web/20130226184036/http://www.huffingtonpost.com/2013/02/25/chinese-hackers_n_2756914.html.

and criminals as a potential explanation. The ODNI Annual Threat Assessment noted that, "of nonstate actors, criminal groups pose the greatest cyberattack threat to the United States."[43] The Government Accountability Office further explained that "criminal groups, hackers and hacktivists, insiders, and violent extremists also pose a threat. These actors have a range of capabilities—from those that use existing tools to exploit known vulnerabilities to organized criminal actors who are highly technical and well-funded professionals working in teams to discover and use new means of attack."[44] Yet, Chinese society possesses little tolerance for this sort of lawlessness. There may exist substantial pockets of entities engaged in criminal cyber behavior originating from within China but is highly unlikely that these entities represent rogue criminals.

There are a limited set of known, and publicly acknowledged, examples of Chinese cybercrime during the COVID-19 pandemic. China was linked to IP theft from several research institutions working to develop COVID vaccines. Analysts tied China to some monetary theft efforts during COVID-19, including financial crimes targeting COVID payment infrastructures. A notable 2022 event included "the theft of taxpayer funds by the Chengdu-based hacking group known as APT41."[45] The Secret Service continued, "it is the first instance of pandemic fraud tied to foreign, state-sponsored cybercriminals that the U.S. government has acknowledged publicly, but may just be the tip of the iceberg, according to U.S. law enforcement officials and cybersecurity

[43] U.S. Government Accountability Office, "Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks," Report to Congressional Committees, June 2022, GAO-22-104256.
[44] U.S. GAO, Ibid.
[45] Sarah Fitzpatrick and Kit Ramgopal, "Hackers Linked to Chinese Government Stole Millions in COVID Benefits, Secret Service Says," NBCNews.Com, December 5, 2022, https://www.nbcnews.com/tech/security/chinese-hackers-covid-fraud-millions-rcna59636.

experts."[46] China is a large country and the potential for rogues exists, but it is more likely than not that most of the rogue-ish, criminal behavior originating from China is the work of state-sponsored or state-supported organizations with an eye toward the theft of American IP that accelerates Chinese research and development and furthers the interests of the state.

Both the federal government and industry cybersecurity experts tacitly acknowledged that these activities were closely linked to, if not outright conducted by, elements of the Chinese government. And in nearly all cases, these events relied on IP-theft, monetary theft, the distribution of misinformation, or other trademark activities associated with the People's Republic of China. The Council of Economic Advisors stated that "Several government and industry sources highlight China's substantial role in cyber-enabled IP theft, asserting that China's 'voracious appetite for information' drives significant hacking activity either from Chinese territory or on behalf of the Chinese government."[47] But most analysts concur that Chinese behavior toward this end tends to be strategic, disciplined, and generally well-regulated by the state, and more often than not advancing the state's national goals and objectives.

While Russia and China both represent a highly capable, motivated, and professional adversary, they do not do so equally. Journalist David Sanger summarized the difference between the Chinese and Russian threat in the following way. "Moscow and Beijing posed distinctly different challenges. Russia was the belligerent disruptor: a

[46] Fitzpatrick, Ibid.
[47] Council of Economic Advisors, "The Cost of Malicious Cyber Activity to the U.S. Economy," February 2018, page 4, https://nsarchive.gwu.edu/media/17664/ocr.

nuclear-armed, financially broken state that sought to divide the West and cause havoc."[48] Sanger continued, "China, by contrast, was a peer competitor focused less on short-term disorder and more on long-term domination. The way to get there, China's leadership was increasingly convinced, was not with nukes or ships but with servers, software, and cables."[49] Without a doubt, China remains America's most substantial global threat on many levels – diplomatic, financial, military, cyber, and more. Yet, the Chinese threat is disciplined, targeted, and strategic in its orientation, something Russia has not been accused of since long before the end of the Cold War.

Tightening the Aperture: Russia

With the elimination of North Korea and Iran as likely culprits, and China less likely given the strategic nature of the Chinese threat and the underlying attack signatures, this leaves Russia as the most likely culprit. Russia, in particular the Russian state, is a complex entity to assess. Following the fall of the U.S.S.R., Russia devolved into a state of lawlessness, something inherited by President Vladimir Putin in 1999 and continuing to this day. Justin Sherman, on behalf of the Atlantic Council, described this challenge the following way. "Broad characterizations of these operations, such as 'Russian cyberattack,' obscure the very real and entangled web of cyber actors within Russia that receive varying degrees of support from, approval by, and involvement with the Russian government."[50] He further described the environment as a "large, complex,

[48] David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (NY: Crown Publishing Group, 2018), 42.
[49] Sanger, Ibid.
[50] Justin Sherman, "Untangling the Russian Web: Spies, Proxies, and Spectrums of Russian Cyber Behavior," Atlantic Council, Cyber Statecraft Initiative, Issue Brief, September 2022, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/untangling-the-russian-web/.

and often opaque network of cyber actors in Russia, from front companies to patriotic hackers to cybercriminals."[51]

The lack of a centralized command and control infrastructure, or a comprehensive national network monitoring and management infrastructure similar to that which exists in China, Russia is a bit of a paradox. Controlled by a strong, nationalistic leader in Putin, and supported by a sophisticated and authoritarian administrative infrastructure, Russia still possesses broad swathes of lawlessness, rogue actors, and independent entities – sometimes of scale – that operate almost autonomously within the Russian Federation. In his Atlantic Council article, Sherman continued, "Contrary to popular belief, the Kremlin does not control every single cyber operation run out of Russia. Instead, the regime of President Vladimir Putin has to some extent inherited, and now actively cultivates, a complex web of Russian cyber actors. This web of cyber actors is large, often opaque, and central to how the Russian government organizes and conducts cyber operations, as well as how it develops cyber capabilities and recruits cyber personnel."[52]

This complex web of actors creates substantial problems with attribution. In a 2011 *Brown Journal of World Affairs* publication author Jason Healey described "a spectrum of state involvement in cyber activity, identifying ten separate types of hacking: state-prohibited, state-prohibited-but-inadequate, state-ignored, state-encouraged, state-shaped, state-coordinated, state-ordered, state-rogue-conducted, state-executed, and state-

[51] Sherman, Ibid.
[52] Sherman, Ibid.

integrated."[53] Unlike China, and most certainly unlike the totalitarian regimes ruling North Korea and Iran, it is entirely possible that in Putin's Russia all ten of these operating models co-exist. The problem with this universe of gradations is, of course, state attribution.

Starting from the top, the Russian government has several entities that are officially engaged in cyber-activities. The FSB, GRU, SVR and multiple smaller entities exist to conduct cyber-operations including offensive, defensive, and surveillance operations in support of the state. Often given a numerical moniker (e.g., Unit 26165, Unit 54777, or Unit 74455), or traditional western nomenclatures (e.g., Fancy Bear, Cozy Bear, Energetic Bear, or Voodoo Bear), these units operate with clear Kremlin support and routinely engage in state-sponsored cyber-activities aimed at enemies of Russia. Conversely, these entities are known by U.S. agencies and their allies, and routinely find themselves the subject of sanctions or indictments for their actions against the U.S. While perhaps not as cavalier as U.S. cyber agencies, whose residence within the confines of Fort Meade include road signs that lead to the front door of the National Security Agency, the Russian units are only slightly less well advertised to the global community.

The pyramid, however, is far from hierarchical and the lawless nature of Russian society provides ample room for enterprises to emerge that can support the goals of the

---

[53] Jason Healey, "The Spectrum of National Responsibility for Cyberattacks," *The Brown Journal of World Affairs* 18, no. 1 (Fall/Winter 2011): 57–70, https://www.jstor.org/stable/24590776.

state, while operating in a less direct fashion. Sherman described this next tier down as "a convoluted web of cyber actors comprised of government-funded front companies, state-tapped individuals, cybercriminals, and 'patriotic hackers,' among others. While some of these entities receive direct orders and financial support from Russian authorities, others have tacit permission to operate independently, so long as they do not upset the Putin regime. The Kremlin's involvement with each of these actors follows a varied and ambiguous pattern of engagement."[54] Once again, this lack of infrastructural integrity and "ambiguous pattern" creates substantial attribution challenges. While independent security event data would clearly indicate that the preponderance of attacks during COVID-19 originated within Russia, the extent to which Russia supported – or was even aware – of these attacks remains an important question.

What we do know about Russian cyber-activities is they tend to follow a particular pattern and leave a particular footprint in their wake. In a post-Soviet Russia, there exist large swathes of over-educated and under-employed individuals capable of supporting sophisticated computing enterprises. To paraphrase Professor Reveron "modern computing is getting easier." Compounding this was a massive rise in criminal activity following the fall of the U.S.S.R. that enabled, or in many cases forced, this populace into computing activities that were criminal in nature. Assuming these entities were allowed to operate because their efforts aligned with Russian state objectives, and the pay represented an opportunity to capitalize on a post-Soviet market economy, it

[54] Sherman, Ibid.

stands to reason that a substantial segment of Russia's highly educated, and poorly employed workforce found their way into cybercrime.

A recent cybercrime alert issued jointly by CISA, FBI, and NSA described the evolution of these entities in the following way:

> "Historically, Russian state-sponsored advanced persistent threat (APT) actors have used common but effective tactics—including spearphishing, brute force, and exploiting known vulnerabilities against accounts and networks with weak security—to gain initial access to target networks. Russian state-sponsored APT actors have also demonstrated sophisticated tradecraft and cyber capabilities by compromising third-party infrastructure, compromising third-party software, or developing and deploying custom malware. The actors have also demonstrated the ability to maintain persistent, undetected, long-term access in compromised environments—including cloud environments—by using legitimate credentials."[55]

This evolution indicates that Russia continues to rapidly evolve its capabilities from unsophisticated attacks, such as brute force exploitation and distributed denial of service attacks, into "persistent, undetected, long-term access" to target computing environments. This sort of evolution suggests several things. First, human capital and talent acquisition to enable such a transformation is no inconsequential undertaking. Finding the talent with the skills, knowledge, and experience to enable this sort of transformation is neither easy nor cheap. Second, capital is required not only to fund talent acquisition and retention, but also the large, sophisticated, and ever-evolving infrastructure necessary to operate a global computing enterprise of this size and complexity. Third, doing so without government discovery, especially in a state run by a

[55] CISA, FBI, NSA, "Joint Cybersecurity Advisory: Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure," January 11, 2022, https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia.

paranoid professional spymaster like Vladimir Putin is highly unlikely. A more likely scenario would be he is not only aware, but directly or indirectly shapes the actions and targets of the entities involved. Justin Sherman argued, "Instead of cracking down, the Kremlin actively cultivated this network of cyber actors, and continues to leverage this ecosystem for purposes that extend beyond criminal activity. The Putin regime allows cybercriminals and patriotic hackers to operate freely within Russia, so long as they focus on foreign targets, do not undermine the Kremlin's objectives, and answer to the state when asked."[56]

Within this complex web of malicious actors exists a toolbox commonly deployed by Russian-linked entities. Ransomware represented the most persistent and effective mechanism by which Russian entities compromise and exploit targeted enterprises. A late 2022 statistical analysis of ransomware attacks from mid-2019 to mid-2022 theorized that "there seems to be some level of loose ties between ransomware groups based in Russia and the Russian government. In that they are criminal organization, they're in it for profit, but it seems like occasionally the Russian government will ask them for favors, and they'll agree to operate on this sort of ad hoc basis."[57] This study supported the release of raw texts from a ransomware insider. Employed by Conti, a Russian ransomware syndicate that analysts believe extorted more than $180 million in 2021, this

[56] Sherman, Ibid.
[57] Lily Hay Newman, "Russia's Sway Over Criminal Ransomware Gangs is Coming Into Focus," Wired.com, November 10, 2022, https://www.wired.com/story/russia-ransomware-gang-connections/.

insider outlined extensive connections between the Conti crime syndicate and the Russian state.[58]

There is ample evidence, including primary, secondary, sensory, intelligence analysis, social media, and other data to substantiate the origin of the malware attacks on the healthcare system during COVID-19. Sensor grid data indicates the origin of malware. Banking data indicates payment recipients, where identifiable. In some cases that will be explored more deeply in subsequent chapters, the culprits were completely transparent about who they were and their intentions toward the compromised. Supporting this trove of data is a short list of actors who have the motive and means to carry out such a brazen and sophisticated series of attacks, at scale, over prolonged periods of time while escaping any sort of culpability or responsibility. While North Korea and Iran possess the motives and means, they possessed a series of hurdles during the COVID-19 pandemic that limited their ability to prosecute such an attack. China, while certainly capable and predisposed to do harm to the U.S. critical infrastructure during the pandemic, does not align with the attack profile and signatures of the perpetrators.

The elimination of these culprits leaves Russia. Yet, as Rid described, "matching an offender to an offense is an exercise in minimizing uncertainty on several levels."[59] The extent to which the Russian state directly or indirectly supported these ransomware criminal activities is difficult to assess. There is almost no scenario where an enterprise

[58] Matt Burgess, "The Workday Life of the World's Most Dangerous Ransomware Gang," Wired.com, March 16, 2022, https://www.wired.com/story/conti-leaks-ransomware-work-life/.
[59] Rid, Ibid, page 7.

of this scale and sophistication operated without knowledge within the highest levels of Russian government. The implications around an oversight of this magnitude are difficult to imagine. The attack profile demonstrated repeatedly during the course of these events is common to the largest of Russia's cyber-gangs and the relationship between the largest of those gangs and senior state leadership is well known and well documented. The outcome of these events – the compromise of sensitive information, the financial exploitation of our healthcare system, and the disruption of care delivery during a time of national emergency – all seem like strategic outcomes of which Putin would approve, if not endorse.

Yet, with all of America's abilities – human, technical, financial, and otherwise – the U.S. remained unprepared. They failed to adequately respond to the COVID-19 pandemic, they failed to secure a critical component of the nation's infrastructure and failed to ensure the physical or cyber resilience and reliability of the segment of American society at its time of greatest need. As Professor Reveron summarized, "we recognize a parallel between the nation's response to COVID-19 and our perpetual inability to respond to cyber-threats at scale in any meaningful and effective way."[60] He continued, "The COVID-19 pandemic, which was predicted but unwanted and ignored, lays bare the national government's capabilities to address a virulent threat inside the country's borders and an inability to protect individual Americans' human security. This same orientation helps to explain the challenge to act when the nation is faced with

---

[60] Derek S. Reveron and John E. Savage, "Cybersecurity Convergence: Digital Human and National Security," *Foreign Policy Research Institute* (August 2020): 556. https://doi.org/10.1016/j.orbis.2020.08.005

incipient cybersecurity threats that individuals, organizations, and corporations face from foreign powers and organized crime.[61]

[61] Reveron and Savage, Ibid, page 556.

Chapter V.

Attacks: By the Numbers

While Russian President Vladimir Putin contended "that the U.S. has yet to show any proof that Moscow was behind the (COVID-19) cyber-attack," there existed ample data from globally trusted sources that these attacks originated within Russian and were highly strategic in their impact.[62] They were focused, timely and effective. These cyber-attacks were more than a minor annoyance to the U.S. healthcare systems. With systems being down across much of the enterprise, healthcare providers operated without scheduling systems, the ability to bill for services, and most critically, without the electronic health records upon which nearly all healthcare care delivery and decision-making relied. The impact can be measured financially, operationally, clinically, reputationally, and especially the burden placed upon already overtaxed nurses and doctors forced to fly blind during critical periods of time. There were a limited number of provable deaths attribute to these cyber-attacks, and substantially more that are presumed to have resulted from the inability of healthcare practitioners to access necessary patient care records or patients unable to access necessary care.

A 2021 cross-industry Ransomware Task Force convened to assess the impact of these attacks and provide recommendations to combat the threat. They summarized these events in the following manner:

[62] Dagen McDowell, et al. "Warning To Russia: Biden To Confront Putin On Cyber Attacks And Election." *Mornings with Maria*, CQ Roll Call, 2021.

> Extensive cyber vulnerabilities across the healthcare industry create potentially lucrative targets for malicious ransom-seeking actors, driving the significant increase in attacks against healthcare facilities. Government policy choices regarding ransomware should focus on this critical threat: statistical analysis reveals that ransomware-driven delays in care in these healthcare systems invariably contributes to a loss of life due to the inability of patients to receive timely care. This illuminates the risk to human life posed by these attacks – and yet the attackers continue to undertake these assaults with near impunity.[63]

While the Ransomware Task Force consisted of practitioners from nearly every industry, they clearly recognized both the vulnerabilities unique to the healthcare system as well as the impact to patient care once those systems were compromised. Regardless of the measuring stick used to gauge the efficacy of these attacks, they were overwhelmingly successful by all measure.

Attack Patterns and Volumes

Historically, the business of cyber-attacks has been less about business disruption and more about the ability to steal monetizable data. Disruption may serve the purposes of a state actor but does very little to advance the interests of criminals who rely on the proceeds of crime to fuel their enterprise. On the contrary, businesses that routinely have difficulty maintaining systems availability and reliability have difficulty staying in business. Hence, this makes them less apt to pay a ransom and, by consequence,

---

[63] Institute for Security and Technology, Ransomware Task Force, "Combatting Ransomware – A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force," April 2021. Of note, the Ransomware Task Force cited Brian Krebs, "Ransomware, Data Breaches at Hospitals tied to Uptick in Fatal Heart Attacks," KrebsOnSecurity, November 7, 2019, https://krebsonsecurity.com/2019/11/study-ransomware-data-breaches-at-hospitals-tied-to-uptick- in-fatal-heart-attacks/, as the basis for attributing deaths to ransomware events.

represent a less attractive target. To use an oft-quoted analogy, "dead men don't pay their bills." Although criminal enterprises are by definition criminal, they are also by definition an enterprise. Hence, without some sort of economic engine to fuel operations they cease to remain a viable going concern. A far cry from the dalliances of computer-literate dormitory scoundrels searching the internet for obscure opportunistic mischief, today's cyber-criminals are strategic, well organized, well capitalized, for-profit enterprises.

Until recently, healthcare proved uninteresting. Basic lack of digitization in the period prior to ARRA proved to be a major hurdle. While seemingly not so long ago, pre-ARRA healthcare operated with a substantial reliance on paper, independent of EHR's, able to deliver care for extensive periods of time with limited to no EHR access. Care delivery may have been slower and somewhat prone to error because of these lapses in data, but this antiquated system possessed inherent redundancies and resilience in the face of attack. If systems were unavailable or proved unreliable, a patchwork of phone calls, faxes, and paper charts routinely proved sufficient to fill in the knowledge gaps necessary to continue to deliver care. Until not so recently, the medical records department in hospitals – complete with rows and rows of paper charts – was commonplace and accessible during EHR outages.

With an EHR mandate embedded within ARRA, this dynamic changed in the years following 2009. Fueled by government subsidies, along with the potential for penalties for non-adoption, hospitals and health systems eliminated the paper charts that hedged against system outages. EHR adoption mandates eliminated the need for, and even the role of, the paper chart in the care delivery ecosystem. Medical records

departments digitized, including the large-scale scanning of historical patient records, and eventually eliminated paper from the enterprise. Unsurprisingly, with the industry-wide adoption of the electronic medical record came a commensurate expansion in the attack surface of the healthcare ecosystem. Post-ARRA healthcare enterprises saw a steady increase in malicious activity. This accelerated substantially during the COVID-19 pandemic. To fully appreciate the implied vulnerability expansion that occurred during the pandemic, it is helpful to better understand the before and after that created such conditions.

First, healthcare records represent a data set that is highly sensitive and personal, but also represents a data set that historically was somewhat difficult to monetize. Compromising sensitive, or even embarrassing, protected health information is not the same as a monetization strategy. Not to mention, a direct-to-consumer monetization strategy would prove impractical to scale. Ransoming individuals for their own healthcare data presents far too many challenges to represent a viable strategy. Second, part of the dysfunction of the modern EHR is its lack of integration and interoperability. While this dysfunction is problematic for users of EHR's, it unintentionally served as a hedge against cyber-attacks. While a cyber-attack may compromise a radiology or lab or pharmacy system, it failed to compromise substantial segments of the rest of a healthcare enterprise. Albeit unintended, stovepiped systems provided a degree of resilience, in that one departments problem failed to impact others. Finally, the scale, dysfunction, and lack of integration commonplace in large healthcare enterprises worked in the favor of the healthcare system. While large, unnecessarily complex, and seemingly unwieldy to internal users of EHR's, it took an outside party considerable time to find monetizable

information. Time is not the ally of the antagonist. Navigating from one information stovepipe to the next caused cyber-criminals to burn time, create noise, and run the risk of discovery in their pursuit of useful data.

ARRA eliminated many of these historical barriers to progress for attackers focused on the healthcare system. Between the passage for the Recovery Act in 2009 and the outbreak of the pandemic in 2019, U.S. healthcare cyber-events followed a steady, unhealthy, but not alarming trajectory. As electronic medical records scaled up in size and complexity, they similarly expanded their exploitation surface area. The U.S. Center for Medicare and Medicaid Services (CMS) reportable events between the passage of ARRA to the outbreak of the pandemic grew at a 46% compounded annual growth rate (CAGR).[64] *The HIPAA Guide* reported a CAGR between 2010 and 2018 of a mere 8% CAGR, finding more breaches in the baseline years of 2010 and 2011 than those reported by CMS.[65] While this sort of growth trajectory is not inconsequential, regardless of the CAGR analysis used it is hardly alarming, nor statistically significant. The rise in cybercrime across all industries during the 2010's proved measurable and generally followed the same linear upward trajectory.

Yet, the pandemic changed this trajectory entirely. Author Jessica Davis described this trajectory, saying "In 2009, the first year of (ARRA), less than 50,000 records were exposed via a data breach; by 2021, the number hit 22.64 million."[66]

---

[64] Office for Civil Rights, U.S. Department of Health and Human Services, "Breach Report Results," https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

[65] https://www.hipaaguide.net/healthcare-data-breach-statistics/.

[66] Jessica Davis, "10 Biggest Healthcare Data Breaches of 2021 Impact Over 22.6 M Patients." *SC Media*, December 21, 2021, https://www.scmagazine.com/feature/breach/10-biggest-healthcare-data-breaches-of-2021-impact-over-22-6m-patients.

According to CMS, between January 2019 and January 2022, there were 1,269 healthcare data breaches that involved 50,161,343 individual patient records exposed during hacking incidents.[67] The resultant CAGR for the period 2009 to 2021 increased to 66%. Depending on whose baseline data you compare the pandemic period against, this represented an increase of roughly 50% against CMS reportable events and more than eight times the baseline reported by *The HIPAA Guide*.

What is particularly remarkable about this period is the intense focus on the healthcare industry, a previously uninteresting business segment that historically lagged most other industry verticals. Emerging from near the bottom of the cyber-incidents industry ranking, in 2021 surpassed finance, the traditional and obvious attack foci to lead all other industries in reportable events. Well regarded law firm Baker Law reported the annual *Baker Hostetler Report*, indicating that by 2022, healthcare was the target of one-in-four cyber-attacks (24%), followed by finance and insurance (17%), business and professional services (15%) and retail (10%). [68] The data proved clear and unambiguous. Following ARRA-subsidized digitization, and accelerating during the pandemic, the healthcare industry proved to be an attractive target, rife with system-wide vulnerabilities, possessing an increasingly complex attack surface, and seemingly unaware of its paradoxical and unfortunate position as both the most critical subsector in the U.S. during the pandemic, yet also the most vulnerable.

[67] OCR, Ibid.
[68] Theodore Kobus, Craig Hoffman, et al., "Baker Hostetler Launches 2023 Data Security Incident Response Report," April 27, 2023, https://www.bakerlaw.com/press/bakerhostetler-launches-2023-data-security-incident-response-report.

Targets

There are several ways to assess, and even prioritize, cyber-attacks during the pandemic period. The U.S. Department of Health and Human Services Office for Civil Rights (OCR) publishes a running list of breaches that impact more than 500 patient records.[69] The OCR Portal, or what is more commonly referred to as the "Wall of Shame," allows anyone to see reportable incidents ranked by geography, entity type, impacted records, type of incident, entity name, and several other sortable data elements. The OCR Portal is the most comprehensive source for data breaches, albeit with some limitations. The 500 patient record limit applies to a specific Covered Entity and much of the healthcare industry remains a cottage industry of small or individual practices. The nature of this industry means that many entities may not have the resources, or even the situational awareness, to identify, acknowledge, or report a breach. There is also the potential for some enterprises to fail to report a breach in a timely or transparent nature. Some of this may be owed to a lack of understanding by members of senior management, the technical details of an event clouding the facts, layers of bureaucracy inherent in large organizations, or in rare cases bad conduct. For these, and potentially other, reasons the numbers reflected in the OCR Breach Statistics are the most comprehensive data set available, yet likely understated.

Breaches are often rank ordered by the number of compromised records, although the Health and Human Services (HHS) OCR method is somewhat obscured by the fact that breaches are reported as allocated to the Covered Entity that effectively has legal

[69] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

accountability for each individual compromised healthcare record. This legal distinction, known as the Covered Entity, defines the legal individual or organization to whom Health Insurance Portability and Accountability Act (HIPAA) laws apply and who is accountable to CMS for HIPAA compliance.[70] For data reporting purposes, this legal distinction creates some ambiguity in understanding underlying causes for data breaches. For example, during the 2020 SolarWinds breach, individual Covered Entities – hospitals, clinics, doctors' offices, insurance companies, labs, and others – reported their individual exposure to the SolarWinds breach, as they were the Covered Entity. However, there is no singular attributable incident to SolarWinds on the OCR portal, as SolarWinds served as a sub-contractor and software supplier to hundreds of Covered Entities required to report the breach individually.

An alternative means of assessing cyber-attacks of consequence would be to focus on entities with substantial brand names. There is a loose correlation between brand and breach significance, as the larger brands tend to have greater exposure to bad actors, yet they tend to have correspondingly larger security budget and resource pool to hedge against that exposure. It is imperfect, but the larger the brand name associated with a breach, the more sophisticated or well-orchestrated an attack is likely to have been. When one reads in the OCR portal about attacks that impact substantial brand names like the Mayo Clinic or United Healthcare, one can assume that the breaches tend to be consequential – sophisticated, strategic, well-executed, and more likely than not the sort of breach that will, or has, occurred dozens or hundreds of times at smaller enterprises.

[70] https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.

Smaller entities present a bit of a paradox, as well, especially when trying to assess lower profile, horizontal attacks across vast swathes of healthcare that may have very little understanding of cyber-attacks or cyber-security. To not be overly burdensome, OCR only requires entities to report breaches in excess of 500 records, and even today much of the healthcare industry remains a cottage industry. According to the American Medical Association, "49.1% of patient care physicians worked in physician-owned practices," and "most physicians (53.7%) still work in small practices of 10 or fewer physicians."[71]

Smaller practices tend to have a substantially smaller overhead structure, including privacy, security, legal, and regulatory resources needed to monitor and report breaches. In some cases, they serve an exceptionally small patient base. In other cases, they serve a patient base in excess of 500 patients but may lack the overhead structure to comply with regulations routinely or effectively. It was never envisioned that small practices would have regulatory overhead structures comparable to their larger peers, but it must be acknowledged that having half of the nation's clinical workforce living and working within the confines of a practice of ten or less physicians represents a substantial data completeness challenge. If more than half of an industry is intended to be somewhat exempt from reporting, yet highly vulnerable – perhaps even more so than their larger peers, there exists an inherent data gap that is difficult to satisfy.

[71] American Medical Association, "AMA Analysis Shows Most Physicians Work Outside of Private Practice," AMA Press Release, May 5, 2021, https://www.ama-assn.org/press-center/press-releases/ama-analysis-shows-most-physicians-work-outside-private-practice.

While statistically interesting, it is not critical to force rank cyber-attacks in some formulaic manner. Healthcare is an industry rife with an unhealthy obsession in the force-ranking of cyber-events and less inclined to act on the output of those assessments. The order or merit is less consequential than what the details of these events allow us to understand. First, it is important to understand the extent to which leading institutions have been compromised, how that compromise was executed, and to the extent practical, by whom. This speaks to the traceability analysis needed to better understand the threat vectors and malicious actors. Second, the means and methods employed provide important details behind the likely culprits for the forensic reasons previously outlined. Third, the relative success of an event provides some insight on the impact of those events on institutions, its workforce, and its ability to deliver timely and accurate care. This latter question around impact will be addressed later, but within the context of healthcare, cyber-events represent canaries in a coalmine for second and third order events that can be life threatening.

Hospitals and Health Systems

In September 2020, Universal Health Systems (UHS) reported an event that devastated the organization. UHS is one of the largest hospital operators in the world with "94,000 employees" distributed across "39 U.S. states, Washington, D.C., Puerto Rico and the United Kingdom."[72] UHS is unique in that it is not only one of the largest providers in the world, it is one of the very few healthcare providers in the Fortune 500,

[72] UHS Investor Overview, June 28, 2023, https://ir.uhs.com.

and even more uniquely operates a global footprint with a visible brand in both the U.S. and Europe. In terms of targetability, there are few better opportunities.

UHS leadership acknowledged in September 2020 they were hit with a ransomware attack and systems would remain down indefinitely. According to trade publications, "the organization was hit with a notorious ransomware strain known as Ryuk. It's just the latest example of the growing cyber threats facing hospitals and health systems already reeling from the impact of the COVID-19 pandemic."[73] Patient care applications remained down throughout September and October 2020, causing the operator to divert patients to other facilities, cancel or delay elective procedures, and substantially scale back the number of available beds for patients. Telemetry and other forms of telemedicine were almost entirely unavailable. The attack impacted UHS well into the fourth quarter of 2020, with UHS leadership acknowledging that "certain administrative functions such as coding and billing were delayed into December 2020."[74] In terms of attack surface, brand exposure, and reportability obligations for a Fortune 500 traded entity, the UHS attack represented a coup d'état.

Scripps Health is the largest and most recognizable healthcare system in San Diego. With more than $3B in revenue and almost 20,000 employees, Scripps is a nearly 100-year-old not for profit healthcare system with hospitals from close to the Mexico

[73] Heather Landi, "UHS Breach Shows the Dangers Facing U.S. Hospitals With Growing Ransomware Threats," *Fierce Healthcare*, October 2, 2020, https://www.fiercehealthcare.com/tech/uhs-breach-shows-dangers-facing-hospitals-growing-cyber-threats.
[74] Kat Jerich, "UHS Breach," Ibid.

border to the southern end of Los Angeles.[75] In May 2021, Scripps Health reported a broad ransomware attack that impacted much of the healthcare system.

According to the San Diego Tribune, "the incident was serious enough to put all four Scripps hospitals in Encinitas, La Jolla, San Diego, and Chula Vista on emergency bypass for stroke and heart attack patients, meaning patients with such life-threatening conditions will be diverted to other medical centers where possible. All trauma patients also were diverted from Scripps Mercy Hospital San Diego in Hillcrest and Scripps Memorial Hospital La Jolla."[76] The attack on Scripps is significant not only because they are one of the largest and most accomplished hospital systems in the San Diego metropolitan area, but options for diversion are somewhat limited. Other than Sharp Healthcare and the UC San Diego Hospitals, there is a precipitous drop off in clinical quality and civilian bed availability when patients are diverted because of a ransomware event.

Attacks were not limited to publicly traded or large regional non-profit healthcare delivery systems. Academic medical centers with recognizable brands proved vulnerable during this period, as well. Yale New Haven Health experienced a ransomware attack via its radiotherapy systems supplier, Elekta. The attack occurred in April 2021, causing

[75] Scripps Health Overview, June 28, 2023, https://www.scripps.org/about-us.
[76] Greg Moran and Paul Sisson, "Scripps Health Targeted by Cyberattack," *The San Diego Union Tribune*, May 2, 2021, https://www.sandiegouniontribune.com/breaking/story/2021-05-02/scripps-hospitals-it-by-it-security-incident-but-patient-care-go.

Yale to divert, delay, or cancel cancer radiation treatments for 200 patients in Connecticut.[77]

The Elekta attack impacted another 170 hospitals and healthcare systems at the same time.[78] The result of this attack had broad implications to cancer treatment. A 2022 article in *Advances in Radiation Oncology* outlined the impact spectrum for the Elekta, and similar, cyber-attacks on cancer treatment. Not unexpectedly, patient impacts ranged from "unacceptable delays in radiation therapy that affect local control, disease progression, and symptom control," to much more severe complications, such as "missed treatment, excessive treatment, and patient harm."[79] As a major supplier to health and hospital systems, the Elekta attack would have impacted the Yale New Haven Health System, including delays, diversions, and the inability to effectively control disease progression amongst this highly vulnerable segment of the population.

In Vermont, the University of Vermont Health Network diverted patients and delayed a large scale EHR implementation because of ransomware activity in late 2021. The *Wall Street Journal* reported "the health network said stress on its networks due to the COVID-19 pandemic, combined with challenges related to the cyber episode, led it to decide to delay the project. Recovery of systems and data is ongoing after the October 28

[77] WTNH, News Channel 8, "Yale New Haven Health able to treat cancer patients again after nearly a week offline due to data breach," *News Channel 8 Online*, April 28, 2021. https://www.wtnh.com/news/connecticut/new-haven/yale-new-haven-health-confirms-its-among-over-40-health-systems-affected-by-cyber-security-breach/.
[78] Ibid.

[79] Michael Oliver, Andrew Pearce, et al, "The Impact of a Cyberattack at a Radiation Oncology Department: Immediate Response and Future Preparedness," *Advances in Radiation Oncology* 7, Issue 5, no. 100896 (September 2022), https://doi.org/10.1016/j.adro.2022.100896.

attack and certain patient care, such as radiology, remains disrupted at some facilities."[80] UVM reported that no patient data had been compromised during the attack, but "ransomware destroyed the computer infrastructure on which the encrypted data resided."[81] Even some eight months later, UVM reported "the network is still working to recuperate after losing upwards of $63 million."[82] For a state with limited diversion alternatives, a highly over-taxed labor force, fiscal constraints, and few relief valves, the University of Vermont Health Network attack proved highly impactful on a regional level.

Smaller, less remarkable, healthcare delivery systems were not immune. In the summer of 2021, St. Joseph's Candler hospital system in Savannah, Georgia fell victim to a crippling ransomware attack. This attack not only forced the system into downtime procedures, or the manual delivery of patient care, but the event exposed the records of 1.4 million patients, one of the single largest breaches during the pandemic period.[83] During the same month, Stillwater Medical Center in Oklahoma and the University of Florida Health Hospitals reported reverting to downtime procedures in response to similar ransomware attacks.[84] In the cases of both Stillwater Medical and the University

[80] Wall Street Journal - Cyber Daily Blog, "Trump Administration Says Russia Likely Behind SolarWinds Hack | Ransomware Attack Exposes Business, Personal Data at Peter Pan Seafoods." *WSJ Pro Online - Cyber Security*, 2021, https://www.wsj.com/articles/cyber-daily-trump-administration-says-russia-likely-behind-solarwinds-hack-ransomware-attack-exposes-business-personal-data-at-peter-pan-seafoods-11609940967.
[81] Jill McKeon, "UVM Continues to Feel Effects of Ransomware Attack," *Health IT Security*, June 24, 2021, https://healthitsecurity.com/news/uvm-health-continues-to-feel-effects-of-ransomware-attack.
[82] Jill McKeon, Ibid.
[83] Steve Adler, "1.4 Million Individuals Affected by St. Joseph's / Candler Ransomware Attack," *The HIPAA Journal*, August 19, 2021, https://www.hipaajournal.com/1-4-million-individuals-st-josephs-candler-ransomware-attack/.
[84] Jessica Davis, "Health Care Ransomware Attacks: Oklahoma Health System Driven to EMR Downtime," *SC Media*, June 16, 2021, https://www.scmagazine.com/news/malware/health-care-ransomware-attacks-oklahoma-health-system-driven-to-ehr-downtime.

of Florida Health, their reliance on downtime procedures lasted anywhere from three weeks to two months until fully recovered.

And even as the COVID-19 pandemic continues to look less like a pandemic and more like an endemic, ransomware attacks on the U.S. healthcare system failed to subside commensurately. As recently as August 2023, healthcare operator Prospect Holdings reported a massive ransomware attack that forced the hospital system to disable the EHR that supports operations across five states. Prospect acknowledged that "elective surgeries, outpatient appointments, blood drives and other services were suspended," and continued that "in Connecticut, the emergency departments at Manchester Memorial and Rockville General hospital were closed."[85] An operator of hospitals and clinics across a five state region, ransomware attacks forced Prospect to deploy the playbook used by so many other healthcare providers, including delays in care, diversion of critical care, and the suboptimal delivery of care for patients already in their stead.

And it would be remiss to not acknowledge that hospitals, health systems, clinics, and other provider assets were not alone during this period. Numerous attacks on healthcare insurers occurred during this period, disrupting payments for care delivery and in some cases causing material damage to the finances and operations of healthcare payers. Point32Health, formerly known as Harvard Pilgrim Healthcare, reported a massive ransomware attack in early 2023, the effects of which the payer had not recovered from by late-2023. In August 2023, Point32 leadership reported a $102.7M

[85] Associated Press, "Cyberattack on Prospect Medical Holdings: Hospitals, Healthcare Disrupted in Five States," *USA Today*, August 4, 2023, https://www.usatoday.com/story/news/health/2023/08/04/cyberattacks-prospect-medical-hospitals-health-facilities/70529098007/.

loss that was characterized as "transient and one time in nature," yet hardly satisfying for management, members, and other stakeholders who rely on the insurers financial solvency to continue to underwrite care delivery for a vast network in New England.[86]

Unfortunately, for the victims of these attacks, there remained little prospect for relief and even fewer prospects for remedy. In many cases, clinicians delivered patient care without access to critical information – medications, allergies, patient history, imaging and lab data, and operational systems that enable the coordination of care across complex healthcare delivery systems. Healthcare payers struggled to meet their payment obligations without the underlying systems necessary to adjudicate and pay claims. According to Emisoft threat analyst Brett Callow "Ransomware is so enormously profitable that, even if Putin were to be able to control Russia-based groups, others would likely continue where they left off." He continued, "Unfortunately, short of banning ransom payments, there's no quick and easy solution to the ransomware problem. Tackling the issue will be a long, hard haul during which time health care and other sectors will continue to come under attack."[87]

[86] Jessica Bartlett, "After Cyber Breach, Point32Health Suffers Financial Losses," *Boston Globe*, August 18, 2023, https://www.bostonglobe.com/2023/08/18/metro/insurer-breach-loss-cost-ransomware/.
[87] Jessica Davis, "Georgia St Joseph's/Candler Health System Shits to Downtime Procedures Amid Ransomware Attack," *SC Magazine*, June 22, 2021, https://www.scmagazine.com/news/malware/georgia-st-josephs-candler-health-system-shifts-to-downtime-procedures-amid-ransomware-attack.

Chapter VI.

Impact Assessment

"The attack on the U.S. healthcare system showed that hackers are singling out hospitals as vulnerable targets."[88]

It is clear from the data, but also substantiated by the benefit of hindsight, that a series of unfortunate events coincided to create a highly combustible situation. EHR adoption exploded, but little consideration was given to securing the infrastructure upon which this now ubiquitous technology relied. Because of ARRA funding, EHR adoption became near-universal, yet the fragile computing infrastructure upon which it relied received no such stimulus funding. In fact, of the substantial list of metrics required to comply with the ARRA mandate and receive funding for the meaningful use of EHR's, only one – a security risk analysis attestation – is reported to CMS. Made even worse, no minimum risk management score is required, only that organizations attest to complying with the conduct of a risk assessment. Compounding this fundamentally flawed architectural approach was a global pandemic that created massive capacity issues for healthcare delivery systems. Overburdened healthcare providers became over-reliant on

[88] Relias Learning, "Cyberattack Almost Shuts Down Health System, Shows Need for Security," *Healthcare Risk Management* 43, no. 1 (2021).

a highly vulnerable computing infrastructure, an unfortunate sequence of events that allowed adversaries of the U.S. to abuse conditions ideal for exploitation.

The Costs

As recently as 2019, investment firm Cybersecurity Ventures predicted that cybercrime was projected to cost the world in excess of $6 trillion annually by 2021, doubling in expense during they six years they assessed cybercrime impact.[89] Yet by the end of the pandemic, this same firm predicted losses would reach $8 trillion by the end of the 2023, representing a 50% increase in cybercrime expenses in only two years.[90] While the cost projection data put forth by Cybersecurity Ventures seems absurdly high, it is not outside the realm of possibility. With the world gross domestic product hovering around $100 trillion annually, it is not statistically impossible that roughly 8% of the world's gross domestic product (GDP) is generated by some form of cyber-oriented criminal behavior.[91] What is even more remarkable, is the concentration of this cybercrime activity in a limited number of countries. If even half the $8 trillion projection is true, the aggregate effect of this activity would represent one of the top-5 GDPs in the world, ranking just behind Japan and Germany.[92]

---

[89] Cybersecurity Ventures, "Official Annual Cybercrime Report (2019)." https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report.

[90] Steve Morgan, "Cybercrime to Cost the World $8 Trillion Annually by 2023," *Cybercrime Magazine*, October 17, 2022, https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

[91] GDP data as reported by the International Monetary Fund, https://www.imf.org/en/Publications/WEO.

[92] GDP ranking data as reported by PopulationU, https://www.populationu.com/gen/countries-by-gdp.

Regardless of what cybercrime loss projections may or may not yield, what does ring true is the substantial increase in cybercrime activity reported during the pandemic. CMS-reported volumetric data collected during this period indicates that cybercrime exploded during the pandemic, directly or indirectly becoming one of the world's largest industries. Not only was event frequency increasing exponentially, but a much more actuarially measurable metric increased at the same time – the cost of individual breaches. According to IBM, by 2021 the cost of a data breach reached an all-time of $9.42M.[93] This number more than doubled between 2019 and 2021, indicating that breaches were becoming more comprehensive, more complex, more disruptive, and more expensive. In even worse news for healthcare, no industry incurred more breach-related expense than healthcare, leading all industries by 2020. According to IBM, the cost of a healthcare data breach was $7.13M, outpacing the energy sector ($6.39M), the finance sector ($5.85M), and the pharma sector ($5.06M).[94]

One of the largest healthcare systems in the world, Universal Health Services, served as a case study in large-scale disruption. In late 2020, UHS leaders acknowledged that "Hackers breached the computer systems for the network of 400 hospitals and care centers across the United States and the United Kingdom, using ransomware that shut

[93] IBM, "Cost of a Data Breach Report," 2022, https://www.ibm.com/downloads/cas/3R8N1DZJ.
[94] IBM, "Cost of a Data Breach Report," 2020, https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf.

down nearly all of the computers."[95] UHS leadership later reported that the financial impact of the cyber-attack cost roughly $67M in lost revenue and remediation expense.[96]

The attack on UHS is believed to be one of the largest and most expensive cyber-attacks on the U.S. healthcare system in history, yet this reported number is likely far short of the total impact to UHS. UHS leadership did not report the indirect impact of the attacks, in the form of workforce attrition, patient safety or care delivery, legal, regulatory, or reputational damage to the health system. The costs for all those intangibles are either difficult to compute, as in the case of workforce attrition attributable to the attack or reputational damage, or long-running, as in the case of legal and regulatory proceedings that may extend over several years. Due to UHS' status as a public company, it served the needs of the company and its shareholders to effectively put a bow on this episode and not unnecessarily prolong a dialogue about this highly disruptive and unfortunate event. Because of this, it is likely that the UHS management calculation on total impact is incomplete and understated.

Who Pays? And How?

There exists a bit of a paradox in the ransomware business model. As previously discussed, it is in the best interests of perpetrators for targets to remain in business. Hence, the new generation of cyber-criminal is forced to walk a fine line between

[95] Universal Health Services, "Statement from Universal Health Services," October 29, 2020. https://bit.ly/2IoCLQp.

[96] Davis, Jessica, "UHS Ransomware Attack Cost $67M in Lost Revenue and Recovery Efforts," *Health IT Security*, March 1, 2021, https://healthitsecurity.com/news/uhs-ransomware-attack-cost-67-million-in-recovery-lost-revenue.

business disruption and business destruction. Should a cybercrime gang expect to get paid, they require a going concern to pay it. However, western nations, and the U.S. more so than others, are not big fans of enabling extortion. In fact, the United States put several limitations on paying ransoms, so much so, that even organizations that may be inclined to pay a ransom may not have the ability to do so. At least not the ability to do so easily or without running afoul of the U.S. government.

Global security firm Crowdstrike conducts a global survey of organizations and assesses several interesting questions beyond a traditional survey. Their 2020 Global Security Attitude Survey found that "27% of victims chose to pay the ransom requested, with small variations at the regional level in terms of average amounts paid." They continued to report that ransom amounts paid ranged from "on average $1.18 million in APAC, $1.06 million at EMEA, and $0.99 million in the United States."[97] Hence, with roughly one in four organizations demonstrating a willingness to pay a ransom, and reported ransom payments hovering around $1 million per episode, cyber-criminals must be judicious in targeting their efforts while simultaneously being exhaustive in their coverage. This data also speaks to some of difficulties associated with ransomware attacks on U.S. healthcare operators, in particular.

Even with its heavy reliance on EHR's, its shaky infrastructural foundation, its massive attack surface, and the criticality of systems to deliver care, hospitals and

---

[97] Michael Sentonas, "2020 Global Security Attitude Survey: How Organizations Fear Cyberattacks Will Impact Their Digital Transformation and Future Growth," *CrowdStrike Blog*, November 17, 2020, https://www.crowdstrike.com/blog/global- security-attitude-survey-takeaways-2020.

healthcare systems still face substantial hurdles to pay a ransom. The Ransomware Task Forced assessed the situation, "A number of factors can influence whether victims agree to pay the ransom demand, including whether they have cyber insurance, the quality of their data backups, and the estimated costs of the system outage. Legal considerations may also come into play: in the United States for example, firms that pay ransoms (and their facilitators) may find themselves in violation of regulations imposed by the Office of Foreign Assets Controls (OFAC)."[98] The U.S. Department of Treasury issued several civil and criminals penalties to organizations that violated sanctions placed on several countries, including Russia, leaving impacted entities with even fewer options to respond to ransomware events.[99] Compounding the legal and regulatory challenges are the technical challenges associated with ransomware payments. Demanding payments via cryptocurrency, for example, presents a technology adoption hurdle for a healthcare system that is aged and antiquated in its financial practices and fluency.

Despite these hurdles, the U.S. healthcare system continues to exhibit some attractiveness. By 2019, the system became hyper-dependent on electronic systems that possessed a higher-than-average consequence of failure. In extreme cases, when systems are unavailable, people die. Hospitals and health systems operate in a highly regulated environment, one that demands transparency in nearly every aspect of its business. There are security and privacy considerations, quality and patient safety considerations, legal

[98] Institute for Security + Technology, "Combatting Ransomware: A Comprehensive Framework for Action, Key Recommendations from the Ransomware Task Force," https://securityandtechnology.org/wp-content/uploads/2021/06/IST-Ransomware-Task-Force-Report.pdf.
[99] United States Department of Treasury, "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," October 1, 2020, https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

considerations, and innumerable other elements of a hospitals performance that are publicly reportable and made widely available. As Professor Rose Bernard summarized, "The criticality of hospital services, combined with the potential for reputational and legal damage, means that hospitals are perceived by threat actors as more likely to meet ransom demands."[100]

Boots on the Ground

A 2020 *New York Times* exposé followed the lives of nurses impacted by the ransomware attack on the University of Vermont Health Systems. Their gut-wrenching stories shone bright what had previously been the overshadowed victims in these attacks – patients and the caregivers trying to treat these patients. While most of the media focused on tangible metrics – number of breached entities, number of records exposed, and the cost of breaches, most of the mainstream media overlooked the most pervasive and human element in these attacks. Patients required care and caregivers were unable to deliver that care. One clinician interviewed during the crisis decried "I have no idea what to do."[101]

Outages in any industry can be highly disruptive. For e-commerce providers, their downtime is measured in second and milliseconds, with a corresponding eye toward revenue loss attributed to slow or unavailable systems. The digital nature of today's

[100] Bernard, Rose, et al. "Cyber Security and the Unexplored Threat to Global Health: A Call for Global Norms." *Global Security* 5, no. 1, (2020): 134–41, https://doi.org/10.1080/23779497.2020.1865182.

[101] Ellen Barry and Nicole Perlroth, "Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack," *New York Times*, November 26, 2020, https://www.nytimes.com/2020/11/26/us/hospital-cyber-attack.html.

banking system demands ultra-high reliability systems with near bullet proof security. Without such assurances, the world's banking infrastructure could prove disastrously unreliable. The consequences of downtime in healthcare can prove even more severe. Noted healthcare author Drexel DeFord explained, "When computer systems go offline, everyone feels the stress of conducting business and delivering care without access to all the information they need. Downtimes are especially dangerous for patients."[102] Few industries can correlate systems unavailability to loss of life as clearly as healthcare.

Even in the best of circumstances, unreliable systems create undue stress on an already overtaxed workforce. This was even more so true during the pandemic. Stress to caregivers creates an unsafe care delivery environment, and an unsafe environment may present dire consequences for patients under the care of those struggling with system outages. The inability to marry up imaging data, pharmacy data, medical history data, patient self-reported data, and clinical orders has the potential to create a deadly care delivery environment for patients. Unavailable or unreliable systems create basic questions around patient identity, patient history, the appropriateness of a medication or procedure, or the opinions or orders provided by other caregivers. The result of these questions is confusion, delay, or in extreme cases patient harm.

Over the course of several months, the attacks on the University of Vermont Medical Center forced the cancelations of surgeries and disruptions to patient care. UVM was forced to furlough or reassign 300 employees as the hospital's networks were taken offline in the midst of the COVID pandemic, and patients were turned away from

[102] DeFord, Drexel. "Sustainable Digital Health Demands Cybersecurity Transformation." *Frontiers of Health Services Management* 38, no. 3, (2022): 31–38, https://doi.org/10.1097/HAP.0000000000000137.

scheduled cancer treatments and other medical procedures. The company's President and Chief Operating Officer estimated the attack would cost roughly $64 million before systems were fully restored. While the direct costs of the event were actuarily assessable, the human toll seemed incalculable. A UVM nurse summarized the experience, saying "To recover from something like this is going to take months and months and months. It feels like we are all alone and no one understands how dire this is."[103]

While UHS management attempted to calm the nerves of the investment community, the outlook on the ground was not as serene. During the attack, UHS management declared, "Given the disruption to the standard operating procedures at our facilities ... certain patient activity, including ambulance traffic and elective/scheduled procedures at our acute care hospitals, were diverted to competitor facilities."[104] Although the playbook for UHS and their predominantly urban hospital footprint allowed for diversion, the outlook for geographically constrained hospitals remained substantially more severe.

A 2021 *Wall Street Journal* article cast light on the very real consequence of ransomware, outlining allegations against the Springhill Medical Center in Mobile, Alabama. A lawsuit, brought by the parents of an infant that died because of delivery complications, claimed a ransomware attack caused hospital staff to miss "troubling signs

[103] Ellen Barry and Nicole Perlroth, "Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack," *New York Times*, November 26, 2020, https://www.nytimes.com/2020/11/26/us/hospital-cyber-attack.html.
[104] Kat Jerich, "Universal Health Services Faces $67M Loss After Cyberattack," *Healthcare IT News*, March 5, 2021, https://www.healthcareitnews.com/news/universal-health-services-faces-67-million-loss-after-cyberattack.

of a baby in distress."[105] The child suffered from umbilical cord asphyxiation and died nine months later due to complications during childbirth. A subsequent Harvard Business School case study raised important questions about the incident, including the extent to which patients should be made aware of cyber-incidents, and the extent to which cyber-incidents have a direct and tangible effect on patient care and quality.[106]

Attacks were not reserved for those with reputable brands, Fortune 500 operators, or large regional integrated healthcare delivery systems. The 50% of healthcare that still operates as a cottage industry experienced similar attacks. A 2022 Medscape article catalogued numerous examples of small and mid-sized physician practices that fell victim to ransomware attacks.[107] Practices as small as two physicians, with unique specializations like ears, nose, and throat were targeted and closed because of their inability to pay and their inability to recover. Seemingly, there existed no rationalization for the targets outlined in the Medscape article, as they ranged in size, specialty, geography, and revenue. The only thing they seemingly had in common was their exposure to the vulnerabilities emerging in the healthcare industry and the concentrated targeting of healthcare practitioners by the assailants.

The combination of ransomware and a pandemic proved a palpable one-two combination. The situation for those providing care proved chaotic. For those that counted the beans, it proved costly. For those attempting to calm public expectations, it

---

[105] Kevin Poulson, Robert McMillan and Melanie Evans, "A Hospital Hit by Hackers, a Baby in Distress, and the First Alleged Ransomware Death," *Wall Street Journal*, September 30, 2021, https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116.
[106] Suraj Srinivasan and Li-Kuan (Jason) Ni, "Ransomware Attack at Springhill Medical Center." *Harvard Business School Case 123-065*, February 2023.
[107] Christine Lehmann, "Docs Refused to Pay the Cyber Attack Ransom – and Suffered," *Medscape*, January 5, 2022, https://www.medscape.com/viewarticle/966051.

proved elusive. And for the patients in need of care – in some cases the most critical of care – it proved dangerous. Syracuse University Professor Lee McKnight, who studies healthcare technology extensively, summarized the situation aptly. He said "I felt sick to my stomach when I learned of the Universal Health Services ransomware attack. Turning hospitals back to 1950s paper-based operations, during a pandemic, will cause people to die despite best efforts and back-up plans. UHS is a huge operation with 90,000 employees now working on their penmanship."[108] Regardless of the complete and final calculus, the healthcare sector suffered greatly, and its impact likely immeasurable because of the myriad ways that cyberattacks adversely affected providers during the COVID-19 pandemic.

[108] Daryl Lovell, "Medical Ransomware Attack Could Spell Disaster, Deaths During Pandemic," *Syracuse University STEM News*, September 29, 2020, https://news.syr.edu/blog/2020/09/29/medical-ransomware-attack-could-spell-disaster-deaths-during-pandemic/.

Chapter VII.

Behind the Numbers: Organized Crime and Russian Support

"A day doesn't go by without news breaking of another healthcare breach, ransomware attack or looming cybersecurity threat."[109]

The average Russian isn't a bad person. In fact, the continuing expression of protest, and even outrage - to the extent such things are allowed in a totalitarian state like Russia – suggests just the opposite. Russian citizens tend to want the same sorts of freedoms and opportunities, balanced by the same sorts of stability and security, as most post-industrial citizens. With some regularity, they express great disdain for a government that, time and again, finds itself on the wrong side of conflicts around the globe. Whether it be in Syria or Crimea, or closer to home within the context of Chechen or even domestic affairs that border on incidents of state-sponsored domestic terrorism, Russia finds itself a global pariah. They have found themselves in the unenviable position of being the lone ally of consequence for several of the world's most totalitarian and despicable regimes.[110]

---

[109] Kat Jerich, "Cybersecurity Roundup: U.S. Agencies Warn of Russian Hacks, Australian Hospitals Struggle to Get Back Online," *Healthcare IT News*, April 27, 2021, https://www.healthcareitnews.com/news/cybersecurity-roundup-us-agencies-warn-russian-hacks-australian-hospitals-struggle-get-back.

[110] A good exposé on the conflict between Russia and Russians can be found in John Sweeney, *Killer in the Kremlin: The Explosive Account of Putin's Reign of Terror* (NY: Penguin Books, 2023).

Yet, the difficulty inherent in Putin's now 24 years in power is discerning between Putin's Russia and Russians. All forms of media, bolstered by western governments, paint Putin's Russia as a homogenous mass, inclined toward the kinds of loosely regulated businesses to succeed the fall of the Berlin Wall – many of which criminal - and not only reticent to replace the regime in power, but seemingly supportive of the status quo. After nearly two and a half decades, separating Putin's Russia from Russians becomes increasingly difficult. If large scale global cybercrime originates in Russia, is it because the society is criminal, is it because the society lacks the resources to effectively police crime, the state actively cultivates these arms-length criminal syndicates as a strategic enabler, or something else? It is hard to say with conviction, creating a paradox for analysts, politicians, and the public alike.

What we can discern with conviction is nearly all roads upon which U.S. healthcare system attacks traveled lead back to Russia. Multi-source data assessments complement one another, suggesting that there is a hub of criminal activity centrally located within Russia. From common source code written entirely in Russian, to shared infrastructure propagating malicious activity, to shared resource pools of talented hackers migrating between employers, to shared banking footprints that reap the rewards of malfeasance, to the admissions, confessions and braggadocio of those engaged in the trade, there is more than ample evidence to clearly indicate that Russia houses, if not hosts, a vast network of cybercriminals who operate with near impunity. To paraphrase an old saying, "there is something rotten in Russia."

There are forensic indicators inherent in any cyberattack. Like DNA left at the scene of a crime, every cyber incident provides useful insights into the perpetrators

behind an event. Accurate and conclusive attribution remains one of the most difficult pieces of the cyber-forensic puzzle and regularly stymies experts in intelligence, national security, law enforcement, and cybersecurity. There are often technical indicators, psychological or human factor indicators, behavioral or pattern indicators, and even secondary or tertiary sources that provide useful clues when trying to develop a comprehensive event analysis. Somewhat surprisingly, cybercriminals tend to be both chatty, sharing their exploits with fellow criminals, and noisy, telling the masses about their exploits. While state-employed actors operate with a high degree of military precision and professionalism, state-sponsored, state-subsidized, or state-acknowledged actors act more like criminals than spies.

In addition to attribution challenges, bad things happen for other reasons. Behind every breach, one will not always find malicious actors. When President Putin claims the U.S. cannot prove Russian support for cybercrime, in some cases this is true. Human error continues to be the root cause of many healthcare cyber events, and for as much as it may seem patriotic to blame Russia or China for the trials of healthcare computing, it is as often a case of our own undoing rather than a malicious actor's doing. As previously discussed, complex systems like healthcare computing are prone to failure, even inside the most responsibly run enterprise. It is also important to note that the big four – Russia, China, Iran, and North Korea may represent the biggest of the big box retailers in global cybercrime, they hardly own the entire mall. Bad actors exist in every corner of the globe, including here at home, and represent some percentage of the overall threat picture and narrative.

What is somewhat shocking, are the lack of insights into the cartels behind much of the cybercrime that impacted healthcare during the pandemic period. Beyond transparency, what is more troublesome is the almost universal absence of ownership demonstrated by the U.S. government in attempting to identify the culprits and to reel in this malicious behavior. There are several announcements from the Federal Bureau of Investigation into these cyber-attacks, warnings and alerts from the Cybersecurity and Infrastructure Security Agency, and frequent phone calls between government agencies and private sector healthcare operators. Yet, this infrastructure did no substantive work following these attacks to thoroughly assess the efficacy of these incidents, their impact, nor to identify the culprits in a more transparent manner. CISA, along with the HHS Cybersecurity Program, publishes incident-specific reports that provide both managerial and technical assessments of attacks against the healthcare ecosystem. Yet, these reports tend to be highly summarized, provide guidance on basic security practices like patching and anti-virus and offer little more than a forensic summary of information already made available through commercial security providers.[111]

Beginning in late 2020, Department of Homeland Security (DHS), HHS, the Federal Bureau of Investigation (FBI), and CISA issued a joint directive indicating they had "credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."[112] Critical to note, U.S. authorities were careful to use the term "cybercrime" when the attack profile demonstrated these attacks continued

[111] An extensive list of the healthcare TrickBot and Ryuk advisories can be found at www.cisa.gov.
[112] Cybersecurity and Infrastructure Security Agency, "Ransomware Activity Targeting the Healthcare and Public Health Sector," October 28, 2020, https://www.cisa.gov/uscert/ncas/alerts/aa20-302a.

to follow a pattern of being less tactical and criminal and more strategic and state sponsored. By early 2021, the recognition of this trend broadened to international audiences when INTERPOL issued a similar warning. "INTERPOL, the international law enforcement organization, issued a statement soon after the COVID-19 pandemic began saying there had been a significant increase in ransomware attacks against healthcare organizations."[113] Yet, with increased recognition, there was little more to help healthcare organizations bearing the burden of these cyberattacks, who concurrently were tasked with dealing with the pandemic.

There may exist, in fact there is likely to exist, a classified body of work to this effect. Given the wall between classified assessments and operations and the private sector, any insights developed from the other side of that wall failed to permeate into the private sector in any meaningful way. But what remains remarkable, given the public nuisance that these events caused, that there were no meaningful government points of view put forward to better assess the state of cyber-security and Russian-sponsored cyberattacks on the U.S. healthcare system. What, specifically, should healthcare entities be doing – and when or to what end, and the extent to which the U.S. government is going to demonstrate some aid or ownership of the problem. Alerts provided by this government infrastructure amounted to little more than your mother's advice to wash your hands before dinner and brush your teeth before bed.

The immutable facts underlying the case leave little to debate. Attacks on the U.S. healthcare system originated within Russia, were deliberate, disruptive, and strategic

[113] Relias Learning, "Cyberattack Almost Shuts Down Health System, Shows Need for Security." *Healthcare Risk Management* 43, no. 1 (2021).

in their timing and impact. They were both noisy and voluminous. They impacted, arguably, America's most critical segment of the infrastructure during a period that the American public relied on that infrastructure the most. Whether the government of Russia supported these efforts, tacitly allowed these activities, or recognized but failed to curtail them is immaterial. They served the strategic interests of Russia, and as such, continued unabated throughout the pandemic. At the same time, our government did little to curtail this behavior and allowed this destructive activity to continue, unrestricted and largely unaddressed, throughout the entire pandemic period.

Culprits and the Criminals

High confidence attribution for cyber-forensics remains a difficult proposition. Beyond the traditional difficulties inherent in cybercrime forensics, there exists the added complexity of criminals and criminal cartels that often fail to remain static, fail to remain cohesive, and in some cases fail to remain tangible. Unlike traditional organized crime syndicates like Cosa Nostra, there is no life-long commitment to the family, nor the traditional structure and governing mechanisms commonplace in other forms of organized crime. These organizations are no less criminal than any other cartel, but the nouveau nature of their crimes gives way to a new way of thinking through the nature of the criminal organization. The comparatively looser fabric of these cyber-cartels demands that U.S. authorities think about them innovatively and develop solutions that are dissimilar to the tools used in the past.

Several criminal cartels operate more like social justice networks than a traditional organized crime family. They identify and recruit young, technically savvy,

disaffected youth, provide them tools and training, and then point those resources toward what they consider socially just ends. While some cybercrime gangs operate as for-profit enterprises, others operate solely on the prospects of fame or recognition within the darker corners of the internet. They may demand some form of tribute, or in other cases may solicit donations to maintain support for the cause. Others have altruistic missions like the group Anonymous. In their case, Anonymous claims to be "no one and everyone at once" and view themselves as "digital superheroes."[114] With the fluidity of the modern cybercrime syndicate, cyber-forensic attribution remains difficult.

There is added complexity in association. It is not only plausible for one criminal cartel to export their exploitation tools and techniques to other organizations, but also becoming almost universal practice. Ransomware-as-a-Service (RaaS) became commonplace in the early 2020's, with more sophisticated cyber-crime syndicates developing software and services that they make available to other less sophisticated criminals. Industry analysts continue to assess the strength of ties between organizations but have found numerous examples of shared or re-used exploitation code, overlapping IP-ranges, and common command and control infrastructure.[115] The extent to which an organization can be definitively linked is difficult when they share virtual attributes like infrastructure, IP ranges, or elements of source code, while they may have little else in common beyond an affinity for cybercrime.

---

[114] Anna Zhadan, "Who Are Anonymous and Why Are They Fighting Alongside Ukraine," *CyberNews*, March 21, 2022, https://cybernews.com/editorial/who-are-anonymous-and-why-are-they-fighting-alongside-ukraine/.

[115] Jon DiMaggio, "Ransom Mafia: Analysis of the World's First Ransomware Cartel," *Analyst1 Whitepaper*, April 7, 2021, https://analyst1.com/wp-content/uploads/2022/09/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLDS-FIRST-RANSOMWARE-CARTEL.pdf.

The replicability of these forensic data points raises obvious questions. Specifically, is this a singular ransomware entity, is this an entity with a cartel-like infrastructure that extends globally, or is this an organization that developed IP and licensed or rented that IP to other cartels who now appear incorrectly affiliated with the perpetrator behind a ransomware attack? Admittedly, the forensic burden on cybercrime is more complex than traditional crime, yet with sufficient noise and volume, attribution conviction is entirely possible.

Creating a financial linkage has been the focus of many FBI, Secret Service, and Justice Department efforts. Following the money trail has been an age-old investigative technique that presents some potential for attribution, yet also possesses some significant limitations. The rise of digital and cryptocurrencies adds complexity into this mix, with digital currency forensics being stymied by the anonymous nature of the digital ledger. Some organizations have gone so far as to establish mediation processes and financial intermediaries to help ensure quick payment and the resolution of services in dispute. For example, industry analyst Jon DiMaggio identified one criminal organization that created a $1 million mediation fund designed to "guarantee affiliate payments, in the hopes of attracting top-quality hackers."[116] Imagine a criminal cartel that serves as a third-party financial intermediary designed to sort out the payment and timeline gap between services procured and services rendered amongst criminal syndicate participants. Today's money trail is increasingly cloudy, complex, difficult to assess, and even more

[116] Dan Patterson, "The World's Top Ransomware Gangs Have Created a Cybercrime 'cartel'," *CBS News Money Watch*, July 22, 2021, https://www.cbsnews.com/news/ransomware-cybercrime-cartel-wizard-spider-viking-spider-lockbit-twisted-spider/.

difficult to prosecute. Hence, attribution via association or affiliation has never been harder.

SolarWinds, SVR, and CozyBear

In the months leading up to the outbreak of COVID-19, the world was reacting to one of the most disruptive, damaging, and widespread attacks in the history of computing. While not directly relevant to the events of the pandemic period, there are several implications from the SolarWinds attack that likely influenced or informed cybercrime during pandemic period. First, SolarWinds was the most ambitious supply chain attack on the global infrastructure executed to date. Rather than identifying and exploiting a definitive target, the SolarWinds breach targeted large third-party suppliers to government, industry, and academia. Rather than successfully executing a breach on a particular target, the SolarWinds hack breached more than 16,000 organizations that employed SolarWinds software.[117]

Second, the attack included two payloads, allowing for multiple exploits of a targeted organization. Ransomware threatened to encrypt and potentially expose organizational data. Should targets fail to pay, threat actors maintained their traditional countermeasure, which is the eradication of encrypted data, or the publication of that same data in the public domain. In addition to these traditional threats, the SolarWinds hack included a second payload that contained a kill switch function that had the potential to shut down organizations that failed to cooperate. Not only did the SolarWinds exploit

[117] Saheed Oladimeji and Sean Michael Kerner, "SolarWinds Hack Explained: Everything You Need to Know," *TechTarget*, June 27, 2023, https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know.

threaten to make data unusable, or publicly publish an organizations data, but they had the second order threat to completely shut down infected infrastructure making recovery nearly impossible.

Third, and perhaps of preeminent significance, the U.S. linked the SolarWinds breach to Russia and official state agencies. As part of sanctions imposed on Russia following the incident, the White House stated, "the United States is formally naming the Russian Foreign Intelligence Service (SVR), also known as APT 29, Cozy Bear, and The Dukes, as the perpetrator of the broad-scope cyber espionage campaign that exploited the SolarWinds Orion platform and other information technology infrastructures. The U.S. Intelligence Community has high confidence in its assessment of attribution to the SVR."[118]

While the SolarWinds timeline predates much of the COVID-19 pandemic, Russia gained valuable insights and lessons learned from its experience with the attack. Supply chain attacks proved highly promising as an attack force multiplier. Why attack a singular organization when the effect of attacking suppliers to hundreds, or even thousands, compounded those effects exponentially? Russia had the opportunity to assess the efficacy of an attack that not only included one traditional threat vector – ransomware – but complemented that threat with additional threatening measures like a kill switch.

[118] White House Fact Sheet, "Imposing Costs for Harmful Foreign Activities by the Russian Government," April 15, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/.

Perhaps the most key takeaway from the SolarWinds experience was the U.S. reaction to the event and the attribution of that event to Russian state agencies. Russia learned a critical lesson about attribution and state sponsorship. While sanctions on Russia during this period were by no means crippling, they were not inconsequential. The U.S. expelled ten diplomats, added six Russian companies to a persona non grata list restricting their ability to work with U.S. companies, and more importantly placed sanctions on the Russian Central Bank and its ability to sell bonds.[119] The U.S. also retained the option to expand those sanctions to Russian sovereign debt, which would introduce long-term liquidity problems. While difficult to assess conclusively, it is not improbable Russia developed a key data point from this exercise. Russia gained a better understanding of U.S. willingness to publish their assessments around sponsorship and attribution, and they better understood the value of having arms-length deniability for similar events in the future.

FIN11

Much like the SolarWinds breach of 2019 and 2020, the largest cyber-security breach of 2021 did not target a specific healthcare provider or payer. Accellion, a popular file sharing platform that allowed entities to securely exchange healthcare data, reported a potential data breach in late, 2020. By mid-2021, Accellion acknowledged an on-going breach that impacted more than 3.5 million records, with large insurers like Centene and HealthNet each having more than one million records compromised. The

[119] Morgan Chalfont and Maggie Miller, "Biden Administration Sanctions Russia for SolarWinds Attack, Election Interference," *The Hill*, April 15, 2021, https://thehill.com/homenews/administration/548367-biden-administration-unveils-sweeping-sanctions-on-russia/.

organization behind this overwhelmingly successful attack was a group known as FIN11.[120]

The U.S. Department of Health and Human Services Office of Information Security published a March 2021 alert that outlined their best assessment of FIN11.

> Mandiant researchers following FIN11 have assessed with moderate confidence that the group operates from somewhere within the Commonwealth of Independent States (CIS), which comprise most of the former Soviet Union countries. This assessment is based on FIN11's avoidance of systems utilizing CIS-country keyboard layouts and the use of Russian-language file metadata. Researchers believe that FIN11 outsources many of their services via underground, criminal communities. This includes using bulletproof hosting services, signed certificates, publicly available malware, and domain registration services. Attribution efforts are hampered when a cybercrime organization uses many of the same publicly available services as other cybercriminals.[121]

FIN11 proved difficult to characterize, primarily by the deliberate efforts to conceal their origin, but also because of their re-use of tools and techniques common to many cybercrime organizations operating at the time. Respected industry journalist Jessica Davis noted in late 2021, "the Accellion hack had far-reaching implications for healthcare." She continued, "The attack was launched by the (FIN11) ransomware group, notorious for actively targeting the healthcare sector. The hacking incident impacted at least 100 companies across all sectors, with the healthcare sector seeing the largest number of victims."[122] CISA confirmed the selective nature of the FIN11 attacks,

---

[120] Tara Seals, "Accellion Zero-Day FTA Attacks Show Ties to Clop Ransomware, FIN11," *ThreatPost,* February 22, 2021, https://threatpost.com/accellion-zero-day-attacks-clop-ransomware-fin11/164150/.
[121] HHS Office of Information Security, "HC3 Analyst Note," Report 202103231400, March 23, 2021, https://www.cisa.gov/sites/default/files/publications/202103231400_Analyst_Note_CL0P_TLP_WHITE.pdf.
[122] Jessica Davis. Ibid, December 21, 2021.

indicating that in addition to their typical high-volume practices they employed a "more targeted approach by operating large scale phishing campaigns and then selecting which of the networks it compromises to target for monetization."[123]

The FIN11 attack demonstrated some notable attributes. Of primary consideration, it proved difficult to assess, with zero clear linkages to the FSB, SVR, or other state sponsored paramilitary organizations. The attack replicated the philosophical approach of using a third-party supplier to multiple entities as a force multiplier. By attacking Accellion, the perpetrators succeeded in compromising hundreds of organizations. FIN11 focused disproportionately on the healthcare sector, a highly relevant strategic shift given the stress COVID-19 began to place on the healthcare system in 2021. Finally, broad, high-volume activity, followed by a targeted exploitation of specific organizations allowed FIN11 to inflict both maximum damage and exploit the most vulnerable and willing to pay of potential targets. A reasonable conclusion from the FIN11 Accellion attack would be that Russia's cybercrime apparatus was learning.

Vice Society

Eskenazi Health System in Indiana suffered an August 2021 ransomware event that impacted over 1.5 million patient records.[124] Industry analysts attributed the attack to the Vice Society who described them as "a Russian-based intrusion, exfiltration, and

[123] HHS Cybersecurity Program HC3 Analyst Note, "CLOP Poses Ongoing Risk to HPH Organizations," U.S. Department of Health and Human Services Office of Information Security, March 23, 2021, https://www.cisa.gov/sites/default/files/publications/202103231400_Analyst_Note_CL0P_TLP_WHITE.pdf.

[124] Carter Barrett, "Eskenazi: Hospital Data Taken in Ransomware Attack," *NPR WYFI Indianapolis*, August 24, 2021, https://www.wfyi.org/news/articles/eskenazi-hospital-data-taken-in-ransomware-hack.

extortion group."[125] While Vice Society historically focused on the education sector, hospitals and health systems have substantial overlap with the education sector, in particular teaching hospitals and health systems. The target profile for healthcare and education are reasonably similar, as well, where large concentrations of data exist for research purposes, information sharing is commonplace, and the attack surface of both education and healthcare institutions can be quite large and unwieldy.

According to a late 2022 CISA Cybersecurity Advisory, Vice Society is not believed to have developed any proprietary or unique ransomware capabilities or variants. Instead, they used commercially available ransomware products and applied that software package to highly targeted environments that Vice Society scouted for prolonged periods of time. After carefully mapping the target environment, they used a combination of existing ransomware software and escalated privileges developed over many months, introduced ransomware to the target and began the extortion process.[126] While Vice Society existed on the public radar targeting the education sector since 2020, in 2022 they diversified into healthcare successfully with the Eskenazi Health attack, suggesting that proximate actors to organizations like FIN11 were beginning to take an interest in healthcare at an inopportune time.[127]

---

[125] Bill Cozens, "5 Facts About Vice Society, the ransomware group wreaking havoc on the education sector," *MalwareBytes Labs*, January 26, 2023, https://www.malwarebytes.com/blog/business/2023/01/5-facts-about-vice-society-the-ransomware-group-wreaking-havoc-on-k-12-schools.
[126] CISA, "#StopRansomWare: Vice Society," CISA Cybersecurity Advisory, September 8, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-249a-0.
[127] Peter Arntz, "Warning Issued About Vice Society Ransomware Targeting the Education Sector," *MalwareBytes*, September 7, 2022, https://www.malwarebytes.com/blog/news/2022/09/authorities-issue-warning-about-vice-society-ransomware-targeting-the-education-sector.

Wizard Spider, CryptoTech and Ryuk Ransomware

Ryuk is one of the most damaging and globally persistent ransomware packages ever developed. Even today, the origins of Ryuk ransomware are difficult to attribute with a high degree of confidence. The source code for Ryuk has been traced back to 2017, but this is an imprecise understanding of its start date.[128] Beyond the mystery of its origination date, the developers behind Ryuk have yet to be identified. Two entities – Wizard Spider and CryptoTech – two similarly opaque cybercrime cartels, are the most likely culprits. However, the precise origins of Ryuk remain unconfirmed. In a cybercrime underworld that prides itself on intangible assets, globally fluid footprints, and the anonymity the modern world of computing enables, these same criminals tend to be voluminous, noisy, and even boastful. There is little consolation in extorting $150 million, as Ryuk has reportedly done, without telling someone about the accomplishment. Somewhat surprisingly, Ryuk remains a bit of a mystery.[129]

One potential culprit behind Ryuk is Wizard Spider. Wizard Spider is a well-known Russian cybercriminal group with a comparatively long history. They are a participant in the TrickBot ecosystem. Dating back to the mid-2010's, TrickBot served as a distribution platform for malware for several years and eluded authorities for extensive periods of time. It often served as a launchpad for different forms of cyber-attacks and different cyber-criminal organizations. Hence, it has been difficult to assess

[128] OnSecurity Team, "Ransomware: A short history of Ryuk," *OnSecurity IO Blog*, November 16, 2020, https://www.onsecurity.io/blog/ransomware-a-short-history-of-ryuk/.
[129] OnSecurity Team, Ibid.

whether Wizard Spider had a hand in the development of Ryuk, or if their TrickBot distribution platform was simply an enabler of Ryuk's propagation to other cybercrime cartels. Unlike other criminal enterprises, like narcotics, there is not a clear delineation between producers, logistical transport, distributors, and retailers. Cybercrime is less well defined. A developer of malware (akin to a drug producer) may also offer that malware as a service (akin to transport and distribution) and may also serve as the attacker exploiting an individual target (akin to a drug retailer bringing a drug to market). For attribution purposes, it is difficult to assess whether an organization like Wizard Spider is engaged in none, some, or all the activities outlined above.

CryptoTech is another Russian criminal outfit, best known for their work to sell a version of ransomware known as Hermes 2.1, something that proved exceptionally damaging to the global banking industry.[130] Hermes is of note because it pre-dated Ryuk, and Ryuk seemingly reused many of the same architectural and coding practices in its source code. It is also forensically interesting to note that Ryuk, when deployed on a machine that was previously infected with Hermes, finds and replaces that code, creating a more difficult to eradicate and well-entrenched piece of malware.[131] What conclusion is to be drawn from this is difficult to assess, but there is clearly some overlap between those with intimate knowledge of the Hermes 2.1 ransomware software and the Ryuk ransomware software, suggesting some sort of correlation between the two parent organizations Wizard Spider and CryptoTech.

---

[130] Jovi Umawing, "Threat Spotlight: The curious case of Ryuk ransomware," MalwareBytes, December 12, 2019, https://www.malwarebytes.com/blog/news/2019/12/threat-spotlight-the-curious-case-of-ryuk-ransomware.

[131] CISA, "Ransomware Activity Targeting the Health and Public Health Sector," *CISA Cybersecurity Advisory*, November 20, 2020, https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-302a.

To make matters even more confusing, it is possible that there is an intermediary in place who is the developer and operator of Ryuk, and criminal organizations like CryptoTech and TrickBot are merely consumers of the product responsible for its distribution and subsequent ransom activities. There is believed to be a great deal of similarity between the Ryuk code sets used by both CryptoTech and TrickBot, suggesting that either there is either a great deal of collaboration between the two entities, or they are consumers of a third party responsible for the development of Ryuk. Distributors of Ryuk are also unique in that they tend to be highly strategic in their operations. Unlike many criminal organizations that are high-volume, low-yield operators who rely on the global numbers game, Ryuk perpetrators tend to be low-volume, high-yield extortionists who demand exorbitant ransoms to unlock encrypted systems. Ryuk tends to be introduced in a highly selective and highly strategic manner, suggesting the cartels behind Ryuk are sophisticated, purposeful, and focused in their work.

Attribution for Ryuk remains a complicated and controversial topic. In a basic attribution assessment, cybersecurity firm Trellix reported "The most *likely* hypothesis in the Ryuk case is that of a cybercrime operation developed from a tool kit offered by a Russian-speaking actor."[132] Beyond this basic understanding of the origin of the Ryuk toolkit, nothing beyond speculation has since emerged as a credible attribution assessment. It is possible, however, that none of these entities are tangible entities. Wizard Spider, CryptoTech, Ryuk, Hermes, and a long list of confusing names with

[132] John Fokker, "Ryuk Ransomware Attack: Rush to Attribution Misses the Point," *Trellix Newsroom*, January 9, 2019, https://www.trellix.com/en-us/about/newsroom/stories/research/ryuk-ransomware-attack-rush-to-attribution-misses-the-point.html.

poorly attributed beginnings could all be an alias for what is believed to be the largest, most dangerous, and most successful cybercrime syndicate on the planet, Conti.

Conti Ransomware Gang

If there were an American organized crime equivalent to global cybercrime cartels, then Conti would be the American version of the Genovese. It is also possible that Conti is so large, complex, and well organized that they may be more akin to the Five Families than a singular organized crime family. Conti is believed by many industry analysts to be the developer and successor organization behind Ryuk, and the current version of what has been a long list of successor organizations. The Conti ransomware line of succession could well include Ryuk, TrickBot, and Hermes and may also be the parent organization to groups like Wizard Spider, CryptoTech and others.[133] Whether it is hierarchical in nature, or more akin to the power-sharing agreement developed by the Five Families decades ago, it is clear that there is substantial connectivity and collaboration amongst crime syndicate members and a demonstrated pattern of cartel-like behavior. What is also clear is the Conti ransomware gang ranks amongst the most powerful and successful of all criminal enterprises, with annualized earnings estimated to be in the hundreds of millions of dollars.

Within the observable universe, there are indications of cartel-like behavior. For example, entities within one gang may compromise a target and supply data to another

[133] Jon DiMaggio, "Ransom Mafia: Analysis of the World's First Ransomware Cartel," *Analyst1 Whitepaper*, April 7, 2021, https://analyst1.com/wp-content/uploads/2022/09/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLDS-FIRST-RANSOMWARE-CARTEL.pdf.

organization for the purposes of conducting an extortion campaign. There is ample evidence of shared code and exploitation techniques, and underground messaging boards acknowledge large-scale cooperation amongst and between cartel members. The Russian invasion of Ukraine provided an unexpected intelligence windfall for western analysts, as Ukrainian hackers who formerly worked within the structure of the Conti organized crime empire extensively published insights into the inner workings of their employer.

A 2022 *Wired* exposé detailed life inside Conti, accompanied by 60,000 messages published from underground message boards detailing everything from recruitment, retention, work life, compensation, targets, techniques, and operational details that would previously have been exceedingly difficult to assess.[134] Conti had grown to such a size and scale that their recruiting efforts employed traditional, commercially-available human resources platforms, their interviewing and onboarding processes were akin to those used by any commercial software development shop, and their compensation schedules were published in an effort to attract and retain the best and brightest in the business. After pouring through the 60,000 posts released by Wired, security analyst Soufianne Tahiri said of Conti, "They operate pretty much like a software development company, and contrary to popular belief it seems that many coders have salaries and do not take part in the paid ransom."[135]

Even within the confines of organized crime, Conti faced the same talent acquisition and retention, resource scarcity, and employee productivity challenges that

[134] Matt Burgess, "The Workday Life of the World's Most Dangerous Ransomware Gang," *Wired,* March 16, 2022, https://www.wired.co.uk/article/conti-leaks-ransomware-work-life#intcid=_wired-uk-right-rail_05a9eccf-45d5-4dce-b5fb-37ab6742d1b9_popular4-1.
[135] Burgess, Ibid.

any other human-intensive, IP-based enterprise faced. Of consequence to the entire world, Russian threat actors emerged toward the latter part of the pandemic as more professional, accomplished, experienced organizations that had substantial capital inflows, efficient operating structures, talent acquisition and retention strategies, and all the accoutrements of a professionally run, yet criminal, corporation.

Collaboration Amongst the Cartels

As if the threat picture could not appear bleaker, the maturity of these cartels was not limited to the individual criminal, nor the tools and techniques they employed. Organizations like Conti and Wizard Spider possessed all the makings of a global software development firm, capable of attracting and retaining the best and brightest workers, employing them toward the development and maintenance of a profitable enterprise, and doing so seemingly beyond the reach of law enforcement. Their fluidity and adaptability made them difficult to pin down and sanctions or other disruptive measures proved little more than negotiable obstacles commonplace in the routine course of business. Yet somehow, for the global healthcare community, things got worse.

Industry analysts assessed that by late-2021 Russian cybercrime gangs reportedly began to collaborate, sharing software, experience, infrastructure, and in some cases human resources.[136] Organizations like Wizard Spider, Twisted Spider, and others demonstrated an unprecedented level of collaboration, often sharing, improving, and reusing ransomware software, creating an even more complex challenge for analysts and

[136] Dan Patterson, "The World's Top Ransomware Gangs Have Created a Cybercrime 'Cartel,'" CBS News Money Watch, July 22, 2021, https://www.cbsnews.com/news/ransomware-cybercrime-cartel-wizard-spider-viking-spider-lockbit-twisted-spider/.

cybersecurity experts. As law enforcement focused on arresting criminals, they did very little to stem the tide of cybercrime. Ransomware gangs seemingly disappeared overnight, relocated, rebranded, and continued their mission nearly unabated.

In May of 2021, the FBI released an alert indicating that Conti was actively targeting the health and public health sector. In March 2022, the FBI, along with CISA, the NSA, and the Secret Service updated guidance on Conti, indicating they believed Conti to be behind more than 1,000 attacks on organizations around the globe. The FBI further confirmed that more than a dozen successful attacks on U.S. healthcare organizations.[137] Perhaps more troublesome, Conti and their extensive network of syndicated hackers, appeared to be collaborating in near real-time on target exploitation.

A December 2021 attack on the Canadian healthcare system reflected a simultaneous attack between Conti and another organization known as Karma. While Karma succeeded in initially accessing the targeted healthcare provider and exfiltrating data, a day later Conti accessed that same provider and encrypted the exploited systems. Hence, one organization effectively stole the data while the other rendered it unusable. This dual-signature attack pattern had not been seen in some years and had attributes like the SolarWinds exploit pre-pandemic. The key difference between 2021 and 2019, by 2021 dual-pronged attacks were being launched by separate organizations working collaboratively, rather than a singular attack, deployed by a single organization, with two malicious software payloads. These attacks were launched by organizations with no clear

[137] Jill McKeon, "Conti Ransomware Group Continues to Threaten Healthcare," *Health IT Security*, March 10, 2022, https://healthitsecurity.com/news/conti-ransomware-group-continues-to-threaten-healthcare.

linkage to the Russian government. For a litany of reasons, including attribution and disruption, this evolution and level of cooperation proved problematic.

Infrastructure sharing is not limited to tools, techniques, intelligence, or even people. The collaboration between these cartels extends to the financial arm of these crimes, as well. Contributing to an even cloudier understanding of the connection between syndicate members, it is known that Ryuk and Conti at times shared the same Bitcoin wallet address for ransom payments.[138] Although it is unclear if these are the same organizations, successor organizations, or organizations operating with a high degree of collaboration, what is clear is they are sufficiently linked that they shared a bank account, which suggests an astoundingly high degree of connection, collaboration, and trust.

Russia, Russians, or Someone Else?

It remains difficult to conclusively demonstrate Russian state-sponsored support for much malicious cyber activity after SolarWinds. It is entirely possible, if not likely, that Russia gained valuable insights from the SolarWinds experience and the sanctions that followed. Russia likely recognized these sanctions as potentially the first step in a slippery slope of unintended negative consequences. If the U.S. could demonstrate high-confidence attribution, it was clear the U.S. would respond. As always, it remains difficult to read the mind of Putin and his public remarks are as predictably measured as they are banal. To paraphrase his earlier comments, "if the U.S. has yet to provide any

[138] Huseyin Can Yuceel and Picus Labs "Leaked Tools, TTP's, and IOC's by Conti Ransomware Group," *Picus Security*, March 4, 2022, https://www.picussecurity.com/resource/leaked-tools-ttps-and-iocs-used-by-conti-ransomware-group.

irrefutable proof, I have no further comment." However, the change in both strategy and tactics following SolarWinds is a meaningful data point.

At the same time, sound assessment rarely relies on concrete information. Both military and civilian threat assessments rely on gradations of uncertainty and conviction, and that pendulum is highly influenced by the data available at the time. What is clear is the fact that these efforts where highly sophisticated in their execution. They were highly targeted and inflicted considerable damage to the sector that the U.S. relied upon the most at the time. Their bounties proved lucrative, and the perpetrators continued to improve in both sophistication and impact. They collaborated extensively, made considerable noise inside a world that is historically quite demure and opaque, and did so with impunity for the entirety of the COVID-19 pandemic period.

In a country that prides itself on its human intelligence apparatus, it is unfathomable that Putin was unaware of these organizations operating large, profitable, capital-intensive enterprises (both human and fiscal) inside the borders of the country he has led for 24 years. His state cyber agencies, alone, would have had ample data to see malicious activity originating within the confines of its global IP address space, and there is no question that both the Russian intelligence and organized crime hierarchies would have been aware of these activities.

Given the scarcity of the resource pool in question, it stands to reason that there is some overlap in personnel who have been employed by government cyber agencies (FSB, SVR, etc.) and private sector entities doing the same sort of work. There is the financial benefit that these organizations provide beyond the disruptive impact they have on Russia's primary strategic adversary. Unlike the FSB, SVR, or other state-supported

agencies, Russian cybercrime syndicates presumably are self-funding. Not only do they not consume money, but they also produce money. Proceeds from ransomware and other data-enabled business models allow these entities to not only self-fund, but presumably kick up money to the official state apparatus that allow their continued existence. Given the hands-in-the-pocket nature of post-Soviet Russia, it is likely that these enterprising corporations and the proceeds they generate for shareholders are viewed as a good thing for the country.

The case for Russian attribution is not foolproof and the prospects of taking a case like this to an American court seem pointless. The facts of the case would be difficult to prove, the evidence would include a nebulous and difficult to trace network of malicious actors, and in all practical terms the actors in question exist well outside of the reaches of western justice. If so inclined, we might convict some number of Russians for cybercrimes, but the prospects of them ever seeing the inside of an American prison are so remote it seems useless to allocate the resource to do so.

At the same time, there needs to be greater conviction in our assessment that Russia enabled a cybercrime empire that preys on American industry, government, and academia, and does so with near-zero consequence. While sanctions applied to Russia following SolarWinds were not inconsequential, the sanctions applied to Russia following the invasion of Ukraine were devastating. The U.S. placed sanctions on Russian banking, trade, entire industrial and agricultural sectors, seized Russian assets from around the world, and put Russia on notice that if it intended to be a participant in global commerce, it needed to leave the newly annexed portions of Ukraine.

Kinetic warfare and cyber warfare do not necessarily demand the same response. While the lines continue to be blurred, there exists today a delineation between a damaging, yet recoverable, event like SolarWinds and the carnage inflicted on Ukraine by the Russian military. Even when the consequences of malicious cyber-activity include the loss of American lives, the response should be measured and appropriate. At the same time, the response should do little to temper or dampen the assessments we conduct, the conclusions to which we arrive, or the level of conviction we present about the crimes and criminals that adversely impacted so many American lives at such a critical juncture in American history. Doing less suggests we lack the analytical capacity to come to more concrete conclusions or we lack the resolve and backbone necessary to stand by those conclusions when they point toward a powerful adversary like Russia. The message either end of that spectrum presents is not acceptable for a world leader like the United States and demands a better response going forward.

Chapter VIII.

The Road Ahead

"That's how a cold war turns into a real war and that's something you want to keep a very good eye on."[139]

When contemplating solutions to the state- or quasi-state sponsored cyber threat, the U.S. needs to contemplate a spectrum of considerations. This is particularly true when threat actors look like rogue elements of a criminal society and less like any sort of formally sponsored organization. Professor Graham Allison describes this potential slippery slope as the "sparks, background conditions, accelerants, and escalation ladders" that present the potential to transition from a non-kinetic cyber-conflict to something materially worse.[140] While his work *Destined for War* focused on the prospect of Sino-American conflict, the framework espoused in that work remains largely applicable to the prospect of US-Russian conflict all the same.

There are historical considerations that create a general pre-disposition toward the Russian state as an untrustworthy, if not outright adversarial party. We routinely view Russian behavior through a Cold War lens, something Putin has done little to dissuade.

---

[139] Philip Seymour Hoffman playing CIA analyst Gust Avrakotos in the movie *Charlie Wilsons War*. https://www.imdb.com/title/tt0472062/characters/nm0000450.

[140] Professor Graham Allison outlined these background conditions extensively in Destined for War, and included a series of conditions present in this study which are too numerous to outline. Graham Allison, *Destined for War: Can America and China Escape Thucydides's Trap?* (Boston: First Mariner Books, 2017), 160 - 173.

While Russia's experience in Ukraine would underscore how unlikely Russia is to be an emerging global threat like China, the combination of their nuclear arsenal and their historical willingness to sacrifice its citizenry to war suggests they are anything but inconsequential. America's strategic tank ditches on its east and west coast are minimized by the proximity of the global internet. Russia, China, and other adversaries are but milliseconds away from critical U.S. infrastructure and capable of scaling their cyber offensive assets in ways, or at a speed, never contemplated in world history. We are closer to conflict with Russian because of this virtual proximity than we have been in all but a few cases since the end of World War II.

The Clausewitzian notion of the fog of war further compounds these historical handicaps. Professor Allison used Clausewitz to argue "three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty."[141] This fog has been true since the dawn of human conflict. Myriad misinformation, misinterpretation, and misplaced assessments led man into conflict in memoriam. Cyberspace exacerbates this problem. It is possible to inflict great harm on a prospective target halfway around the world while exposing little more than a temporary digital footprint that may or may not be indicative of the actor behind the attack. As Professor Allison described, "compared with the bluntest instruments of war, especially nuclear bombs, cyberweapons offer the promise of subtlety and precision. But this promise is illusory. Increased connectivity among systems, devices, and "things" creates a domino effect."[142] The reach and speed of cyberconflict creates difficulty understanding the

[141] Carl von Clausewitz, *On War*, ed. Peter Paret, translated by Michael Eliot Howard (Princeton, NJ: Princeton University Press, 1989), 101.
[142] Allison, Ibid, page 165.

nature of an attack. A lack of attribution compounds that speed. Interconnectivity and the potential for collateral damage maximize the impact. Hence, we likely have never encountered a more dangerous set of sparks, conditions, accelerants, or ladders than we encounter today.

Starting from the Top

Recently, President Biden issued budget guidance to all federal agencies prioritizing cybersecurity, stating "the administration is committed to mounting disruption campaigns and other efforts that are so sustained, coordinated and targeted that they render ransomware no longer profitable."[143] The same budget prioritization continued "Budget submissions for departments and agencies with existing, designated roles in the disruption of ransomware should demonstrate how they: prioritize staff to investigate ransomware crimes and disrupt ransomware infrastructure and actors; prioritize staff to combat the abuse of virtual currency to launder ransom payments; and ensure participation in interagency task forces focused on cybercrime."[144] At least from this communication, it would seem that the chief executive is focused on the nation's cybersecurity and mustering resources to counter the alarming trends seen in the past.

Yet, a global security survey released by industry leader Sophos at roughly the same time revealed that "average (mean) ransom in 2023 was $1.54M. This is almost

[143] Jonathan Greig, "White House Outlines Cyber Budget Priorities, Including Making Ransomware 'No Longer Profitable,'" *The Record Media*, June 28, 2023. https://therecord.media/white-house-cyber-budget-priorities-making-rasomware-not-profitable-zero-trust.
[144] Greig, Ibid.

double the 2022 figure of $812,380."[145] The number of organizations (66%) indicating they had been the target of a ransomware attack remained the same as the prior year. In purely financial terms, this would indicate that the size of the global ransomware market roughly doubled between 2022 and 2023 indicating that whatever measures or countermeasures the U.S. deployed during this period had no effect on ransomware market growth. We are dropping pebbles in the ocean, yet hardly creating a ripple and clearly resulting in no measurable effect.

Across the pond, the story is no different. In the same month as President Biden's directive, the U.K. National Health Service (NHS) reported the largest ransomware attack in NHS history. Barts Health, the NHS administrator for five London hospitals serving more than 2.5 million patients acknowledged a massive ransomware compromise. The release went as far as to acknowledge the nature of the ransomware attack and the culprit (the BlackCat ransomware gang) providing uncharacteristic timeliness and transparency in their official statements.[146] This level of immediacy and transparency may signify a shift in the joint U.S./U.K. response to a common enemy.

It is believed that BlackCat is a derivative group of DarkSide, an organization responsible for the 2021 Colonial Pipeline attack. The Colonial attack represents one of the first known examples of the U.S. deploying offensive capabilities to interdict both the computing infrastructure of a malicious actor and targeting the financial backbone supporting the operation. In the Colonial case, DarkSide ceased operations after

[145] Sophos, "Ransomware 2023," *Sophos White Paper*, May, 2023, https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf.
[146] Carly Page, "UK Battles Hacking Wave as Ransomware Gang Claims 'Biggest Ever' NHS Breach," *TechCrunch*, July 10, 2023, https://techcrunch.com/2023/07/10/uk-hacks-public-sector-nhs-ransomware/.

acknowledging on underground message boards that both their computing operations and financial infrastructure had been destroyed.[147] The UK response to the NHS attack may have been a similar warning shot across the bow, and intended to advise the culprits that we are both aware of, and willing to target, those responsible for cyberattacks against the healthcare infrastructure.

Yet, given the lengthy history of unchecked cyberattacks, we should be well beyond warning shots, transparency, and calls to action. After decades of unimpeded bad behavior, and more immediately a demonstrable pattern of disrupting or destroying America's ability to deliver care safely and reliably during the COVID-19 pandemic, U.S. citizens deserve a more deliberate, actionable, and accountable plan. The country demands a more empowered cyber leader who can marshal resources to help protect critical infrastructure assets and do more than issue plans and establish priorities that find themselves consistently deprioritized, underfunded, or outright ignored. There also need be serious consideration given to what sort of quasi-governmental activities or infrastructure would allow for more proactive interventions without attribution to the U.S. government or the citizenry they represent.

If the size (defined by cost) and scale (defined by number) of cyber events continues to rise, while malicious actors simply pack up shop, move down the street, rebrand, and resume their activities, what can we say has been done? We've failed to change the slope of the threat curve. We've failed to dissuade malicious actors from engaging in cybercrime against the U.S. critical infrastructure. We've failed to protect

[147] Center for Internet Security, "Breaking Down the BlackCat Ransomware Operation," *CIS Blog Posts*, https://www.cisecurity.org/insights/blog/breaking-down-the-blackcat-ransomware-operation.

the underlying critical infrastructure assets. What can be pointed to between President Clinton's issuance of PDD-63 in 1998, a seemingly monumental event that prioritized cybersecurity as a national imperative, and today some 25 years later where the data would suggest that the problem is bigger, more pervasive, more damaging, and less checked than at any time in history? The U.S. demands a more deliberate, aggressive, and accountable response.

From Advisor to Owner

The senior most U.S. cyber executive has been an executive in name only for more than two decades. With the appointment of the first tranche of cyber advisors to the President, eventually being characterized as "cyber czars," this role has largely been as ineffective as it has been illusory. Even with the strong budget guidance issued by the Biden administration, that guidance made no mention of centralizing the leadership, accountability, or execution of the cybersecurity mission. In fact, it referred to a state of continued cooperation and collaboration amongst "interagency task force(s)" which suggests an operating environment more akin to the status quo than a sea change in America's approach to the problem.[148]

Beginning with Richard Clarke and Howard Schmidt and continuing to present day, this role has done little to advance our nation's cybersecurity posture. They've done a commendable job raising awareness. Yet, successive iterations of security strategies, implementation plans, cybersecurity frameworks, and Presidential Decision Directives

[148] Jonathan Greig, "White House Outlines Cyber Budget Priorities, Including Making Ransomware 'No Longer Profitable,'" *The Record Media*, June 28, 2023, https://therecord.media/white-house-cyber-budget-priorities-making-rasomware-not-profitable-zero-trust.

have done nothing to move the needle. This role proved so impotent; President Trump eliminated the position altogether. National Security Advisor John Bolton argued that eliminating this position removed an unnecessary layer of government bureaucracy.[149] The data before and after the elimination of the cyber czar proved no different, suggesting that the role as previously constructed proved immaterial in the fight against cybercrime. While the Biden administration may contend that the trend line during the current administration is one inherited from its successors, and measures taken within the current administration will bend that curve, the jury remains unseated. Time will tell.

Starting with the President, the U.S. requires executive leadership and an informed, engaged, somewhat technically competent chief executive who remains as conversant on cyber warfare as he or she is on kinetic warfare. Few modern American leaders possess any sort of diplomatic or strategic military acumen, but they learn these skills in the earliest days on the job. They are often surrounded by the best and brightest minds in the business working either directly for, or directly advising the President of the U.S. This has been true since time immemorial on topics like the economy, diplomacy, and war, and should be no less true today on cyber.

The days of the U.S. President being unengaged or uninitiated in cyber security are behind us. While unreasonable to expect every President to have a consistent level of cyber-competence, it is reasonable to expect that they would lean into this topic and develop some basic levels of competence in the earliest days of their administration. If

---

[149] U.S. CYBERSECURITY PREPAREDNESS AND H.R. 7331, THE NATIONAL CYBER DIRECTOR ACT, Hearing before the Committee on Oversight and Reform, House of Representatives, July 15, 2020.

you consider the risk calculus of probability times impact as a simple ordering mechanism, there is an exceptionally high likelihood of a major cyber-event within their administration, and the potential for that event to have catastrophic consequences are reasonably high.

President George W. Bush, a person routinely derided by his critics for his folksy humor and the casual way he conducted presidential business, was exceptionally committed to this risk assessment, risk mitigation, and risk preparedness regimen. While reasonably well-read in nuclear, kinetic, and cyber-conflict, he believed neither he, nor the country, were prepared for biological events. He was the first President to commit substantial resources to planning and preparation around a pandemic event. He proactively engaged experts from academia and industry to raise his administration's awareness and promote efforts around biological preparedness. Unfortunately, as we learned during COVID-19, this represented a momentum that subsequent administrations failed to maintain.[150] Whether the risk calculus be biological, cyber, nuclear, or other threats, it is not only possible, but critical that each successive administration lean into these critical risk management priorities with the strongest conviction. The potential for an event too high and the consequences of an unprepared nation too severe to accept anything less than a full commitment to presidential leadership and a holistic commitment to nationwide cyber risk preparedness.

[150] Matthew Mosk, "George W. Bush in 2005, 'If We Wait for a Pandemic to Appear It Will Be Too Late to Prepare,'" *ABC News*, April 5, 2020, https://abcnews.go.com/Politics/george-bush-2005-wait-pandemic-late-prepare/story?id=69979013.

Creating a Singular, Accountable, Executive Leader

The U.S. requires an empowered, funded, and accountable executive to lead cyber for the nation. This person is no longer a Presidential advisor nor cross-community coordinator. Although advising the President and coordinating community response will be part of their role, this role should own federal cyber monitoring, cyber defense, and cyber response activities. Even today, the consolidation of civilian accountability for national cyber-defense continues to remain a controversial and heavily debated subject. The Department of Justice argues that they need unique cyber capabilities for the investigation and prosecution of cybercrimes. Treasury argues that the protection of the U.S. monetary system is something uniquely proprietary to their department and not something to be allocated or outsourced to another entity. Health and Human Services historically presents few such arguments about criticality or propriety, yet no agency would assume an unfunded mandate as vast and complex as protecting America's healthcare ecosystem, still representing nearly 20% of our nation's GDP. In all but the Department of Defense, there exists a massive void in ownership, which speaks volumes to outcomes.

The Department of Defense, arguably the single agency with a defensible argument about the proprietary, critical, and unique nature of their mission statement, addressed this problem over the last several decades. While multiple agencies worked the cyber mission for the Department of Defense prior to 2009, the U.S. Cyber Command serves this capacity today. The National Security Agency, as an example tenant command, provided exceptional cyber offensive, exploit, and defensive capabilities over

several decades prior to the establishment of Cyber Command. Today, the head of Cyber Command concurrently serves as the head of the National Security Agency and chief of the Central Security Service, an alignment that removed all ambiguity about who is on point for cyber defense, exploit, and offense for the Department of Defense. Similarly, cyber-tenant commands from across the services were reassigned to support Cyber Command, providing a replicable model for other civilian departments to emulate.

It could be argued, that due to the limitations demonstrated by the current status quo amongst U.S. civilian agencies, the Department of Defense U.S. Cyber Command should consolidate this function universally and own cyber responsibilities for the entire U.S. government. Some of the foundation toward that end has recently been laid. Historically, the Cyber Command mission statement focused on "the operations and defense of specified Department of Defense information networks." Yet in 2022, Cyber Command acknowledged "Recent high profile cyberattacks and operations, such as the state-sponsored data breaches within the Office of Personnel Management or the SolarWinds attack, illustrate cyberspace can no longer be treated as a separate and lesser category of national security, but must be dealt with as a strategic element of national power."[151] Presumably, this acknowledgement expands the aperture on the cyber domain to extend well beyond those networks built and maintained by the Department of Defense. Should this leadership role be assumed by the DoD is debatable. They clearly have sufficient threats and vulnerabilities to work through from China, Russia, Iran, North Korea, and dozens of other countries, in addition to homegrown problems, to keep

[151] U.S. Cyber Command PAO, "Cyber 101 – U.S. Cyber Command Mission," October 18, 2022, https://www.cybercom.mil/Media/News/Article/3192016/cyber-101-us-cyber-command-mission/.

them busy. Ownership for the civilian mission might represent a bridge too far. What is undeniable is the need to centralize and professionalize the cyber capabilities of the nation and provide accountability where no such accountability exists today.

Office of the National Cyber Director

In response to the Trump administrations elimination of the cyber czar position, Congress established the Office of the National Cyber Director (ONCD) in 2021. The ONCD "advises the President of the United States on cybersecurity policy and strategy."[152] While this represents progress, it also provides the false allusion that the United States is taking the cybersecurity mission more seriously than it is in practicality. While tasked with coordinating a "whole government approach" to cybersecurity, the office serves largely as the principal author and architect of the nation's cybersecurity strategic plan, while advising elements both up and down the chain of command on how to prioritize resources to accomplish that mission.[153] It is unclear how different this role is intended to become from the ineffective figureheads that filled this void previously. At least optically, this simply is not enough.

Should the ONCD be the right apparatus to marshal the non-national security assets of the nation, it must substantially broaden its aperture. The ONCD needs be positioned to employ native cyber capabilities – defensive, offensive, and exploit. These assets should not be capabilities coordinated with or borrowed from other government agencies, but capabilities native to the ONCD, under its direct command and control, and

[152] White House PAO, "Office of the National Cyber Director," https://www.whitehouse.gov/oncd/.
[153] Ibid.

employed according to the doctrine espoused in the National Cyber Security Strategy. Borrowing a construct developed by the Department of Defense, the ONCD needs to extend its visualization of the cyber threat picture, the cyber battlespace, and proactively engage threats actors to disrupt their actions before they materialize on the U.S. shore. It needs to be resourced by the redundant and ineffective assets currently being squandered across a broad swathe of government bureaucracy and operated as a singular, cohesive unit. In the most practical of terms, if we want our nation to act like we take the cyber threat seriously, identifying a singular leader and supporting that leader with streamlined, capable, and focused resources is the first and most critical step in achieving the desired outcomes.

Consolidating Resources

While myriad challenges exist in this consolidation and rationalization effort, there are small armies of professionals who do this sort of work every day. The practical details around execution should serve as no impediment to progress. Corporate mergers and acquisitions, supported by post M&A integration teams, are highly effective at the consolidation and normalization of integrated assets. It is not particularly difficult to put a veritable rope around all your assets, to eliminate and lean out redundancies, to point the best and brightest of those who remain at a new mission statement, and to coach that team up to perform over some period of time. Far too often, we find ourselves stymied by the complexities of action and by default revert to inaction. The events of 9/11 point to the risks associated with inaction, yet the events that followed are clearly indicative that America is more than capable of working through the integration challenges of

standing up a more integrated, less redundant, and more accountable department during times of need.

Armed with the right organic capabilities, the Office of the National Cyber Director should have ample cyber intelligence gathering and analysis assets to understand the threat picture in a much more robust and comprehensive manner than today. These assets need not be net new, but rather an aggregation of the landscape of quasi-effectual cyber analysis and cyber defense assets sprinkled throughout government. By consolidating these human resources, it is more likely than not that the level of professionalism would rise as higher performing resources from across the cyber-ecosystem assume greater responsibilities and have the autonomy to separate the proverbial wheat from the chaff. Not only would they have the autonomy to do so, but they would also have the mandate to do so. Today's construct of having underperforming, redundant, sector-specific capabilities embedded within individual agencies creates a broad landscape of problems.

First, there is inherent inefficiency in redundancy. This redundancy is coupled with huge variation in competence and sophistication across the sectors. While having some sector-specific expertise presents utility, it would be no different than having a specialized industry desk within a cyber-operations center the same way operations centers have different geographic or topical experts consolidated under one roof. The intelligence community does this today. The cyber community could emulate this model with ease. Second, information sharing between industry and its regulator presents substantial barriers to collaboration and transparency, a problem that confronts several information sharing and analysis centers today. Separating the regulating agency from

the cyber-protection agency solves for this problem. Third, the patchwork of government entities engaged in cybersecurity operations remains perpetually problematic. It is unclear whether an issue is owned by entities like the ONCD, the Department of Justice, the U.S. Secret Service, a sector-specific agency (e.g., Department of Treasury, Department of Energy, or Department of Health and Human Services), state or local law enforcement, left to private industry, or a matter that rises to the level of intervention by the national security apparatus. As cybersecurity recently emerged as a national security strategic imperative, knowing who is on point has become less, not more, clear from the latest National Cybersecurity Implementation Plan.

Shrinking the Threat Picture

While the consolidation and centralization of non-DoD cyber operations solves part of the problem, it does not solve all the problem. The threat picture remains unchanged, only the response infrastructure is different. Inside this infrastructure are innumerable legal, regulatory, diplomatic, or other barriers that prevent the ONCD from becoming as effective an entity as the NSA. Provided with substantial latitude following 9/11, the National Security Agency and the U.S. Cyber Command enjoy a level of latitude that is unrealistic for a civilian agency absent a 9/11-like event. The National Security Agency possesses substantial offensive cyber capabilities, that while generally kept in reserve, find themselves employed in a limited number of known cases. Similarly, if the U.S. is serious about its intent to disrupt cybercriminals, the civilian cyber executive will require access to comparable offensive cyber capabilities.

ONCD should contemplate a purpose-built organization that addresses this need, something akin to the way the U.S. employs Academi – formerly Blackwater. A cyber-private contractor would serve several purposes. First, it is likely that a private entity would move faster and prove more successful in recruiting and employing a sizable cyber workforce. Second, given the dynamic nature of the threat, a private contractor would be capable of employing the same sort of deft geographic anonymity and fluidity we confront from our adversaries every day. Third, private contractors are less constrained by rules of engagement, in particular when operating from a remote, or loosely regulated nation, and conducting operations against an adversary located in a similarly loosely regulated nation. Should Russia object to the remote curtailment of criminal behavior within its borders – especially when Russia denies all knowledge or connectivity to the activity or actors – then there is lesser ground for the Russian state to object to attacks against those criminal elements. Finally, private contractors provide a layer of plausible deniability. While this layer of protection has practical limits, it is a cloak behind which our adversaries hide with great regularity, and as a policy option should not be discounted.

Building – *and Implementing* – a Better Plan

Even acknowledged within PDD-63 25 years ago, there remains broad recognition that most of the nation's critical infrastructure is owned by the private sector. Explosive technological growth experienced during the 1990's tipped infrastructure ownership out of the hands of government and academia and into the hands of private corporations and private citizens. Massive and global technology propagation made it impossible to apply the normal tools of government to minimize risks inherent in broad

tech adoption. Regulation, legislation, sanctions, taxes, and subsidies became impractical when one considers the speed and rate of technological change during this period. The speed of action demonstrated by most federal, or state governing bodies could not hope to keep up.

PDD-63 recognized the criticality of private sector engagement and called to action elements of the public and private sectors to organize and collaborate in meaningful ways.[154] The National Infrastructure Advisory Council assembled leaders from the nation's critical infrastructure sectors to advise the President of the U.S. on critical infrastructure protection efforts. Sector-specific Coordinating Councils were designed to serve as a communication and collaboration vehicle for the exchange of relevant threat and vulnerability information, and the coordination of incident response efforts. And while pioneers like Richard Clarke pride themselves on drafting "the first national cybersecurity strategy that the nation ever published," there is little in the data to demonstrate that this strategic framework has been anything other than an ineffective panacea that proved wholly futile in preventing the sorts of attacks demonstrated during the COVID-19 pandemic.[155] In some cases, the limitations were structural while others they were personal or political, but our nation's "cyber czars" have done little to move the needle on the country's overall cybersecurity posture.

---

[154] The White House, "Presidential Decision Directive – 63," Washington, D.C., May 22, 1998, https://irp.fas.org/offdocs/pdd/pdd-63.htm.

[155] Richard Clarke's overstated claims can be found in his book Richard A. Clarke and Robert K. Knake, *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats,* (NY: Penguin Press, 2020), https://www.amazon.com/Fifth-Domain-Defending-Companies-Ourselves/dp/052556196X.

To compound the inefficacy of these early efforts, it is important to note that the current Office of the National Cyber Director published a revised National Cybersecurity Strategy, overhauling much of both the thinking and policies put forth by prior administrations. They released an accompanying National Cybersecurity Implementation Plan (NCSIP), something that has been done sporadically in the past, as well. The NCSIP outlines a series of tangible, tactical, impactful measures to meaningfully reduce the cybersecurity threat to the U.S., something that prior iterations of government failed to either develop, failed to execute, or both.[156] While a promising start, to paraphrase an old proverb, the road to better cybersecurity is paved with good intentions. Only time will tell if this administration is any less ineffective in its implementation efforts than its predecessors.

There are aspects of the National Cybersecurity Implementation Plan that look promising. Commonplace to its predecessor efforts, the NCSIP addresses criticisms that the government continues to have "a vision without a plan."[157] In particular, the more proactive orientation of the Plan is a marked departure from prior iterations that focused exclusively on defensive threat countermeasures. The Plan argues that the U.S. should be proactive in its efforts to interdict malicious cyber actors and put in place countermeasures that make activities like ransomware unprofitable. While this orientation pivot is promising, it is accompanied by a typical bureaucratic malaise of improved regulation, enhanced public-private sector collaboration and information sharing, hiring more lawyers to focus and advise on these operations, and the usual

[156] Trey Herr, Stewart Scott, Maia Hamin, et al, "The National Cybersecurity Strategy Implementation Plan: A CSI Markup," July 18, 2023, https://dfrlab.org/2023/07/18/national-cybersecurity-strategy-implementation-plan-markup/.
[157] Ibid.

multitude of bureaucratic hurdles that slow, if not abort, these efforts before they ever get started. The layers of the NCSIP dedicated to dealing with barriers to progress – namely legal, regulatory, or policy considerations – should speak volumes to the need to reconsider alternative solutions like a private contracting solution that circumvent many of these issues.

It is difficult to fathom that between the release of PDD-63 in 1998 and the publication of the current NCSIP twenty-five years later that so little tangible progress has been made. This is most certainly to the detriment of American citizenry. Each administration is afforded a do-over, of sorts, but time has never been the ally of inaction. To become effective, or even credible, there remains a great deal the ONCD still needs to do. Beyond consolidating and professionalizing the cyber-defense capabilities of the government, improving information collection and analysis capabilities, and building out partnerships who can help extend America's cyber-reach, much of the work to engage the private sector remains. The private sector will represent the largest vulnerability in this tenuous calculus for the foreseeable future. Not only is the private sector the owner and operator of most of the nation's critical infrastructure, but they also remain highly reluctant to accept further regulation, dissuade oversight, and have a generally high tolerance for failure. Like the rest of America, the risk-reward calculus must tilt toward the catastrophic before there is a broad call to action, something unique to American business. Addressing the private sector component of the problem remains critical, if not paramount, and consideration must be given to how best to mobilize this otherwise distracted component of the solution.

Mobilizing the Private Sector

If our nation's critical infrastructure is disproportionately owned and operated by the private sector, engaging the private sector becomes paramount. The absence of a catastrophic event has the unfortunate consequence of suggesting that the conditions that enable a catastrophic event are not present. Industry routinely takes comfort in the absence of catastrophic events, or in some cases the ability to recover from near-catastrophic events, thereby reinforcing the notion that things may not be as bad as the headlines suggest. This could not be further from the truth.

Understanding private sector motivations is an important consideration. As the Stanford Health Chief Security Officer Michael Mucha stated "telling us we need to do better is simply not going to get it done. Most healthcare systems operate at a loss, and the few of us that are not losing money have a long list of other priorities, mostly focused on patient care. There needs to be some sort of risk-reward framework that causes the industry to focus on this for an extended period of time."[158] His commentary is not without logic. Economic fundamentals in healthcare are tenuous, at best. Few health systems today operate profitably, and many are living off both borrowed money and borrowed time. For those with means, direct patient care investments merit priority. Cybersecurity is difficult to understand and assess, hence difficult to prioritize. How much should one pay for insurance for an event that may or may not materialize? There also exists the false conclusion that despite all the bad things happening around an entity, few ever shutter their doors. Maintaining a heightened sense of awareness, an investment

[158] Michael Mucha, interview with Scott Blanchette, June 23, 2023.

priority, and doing so over sustained periods of time is unlikely in an environment where institutions are often unable to make payroll.

The private sector has proven adept at operating in an environment where incentives and penalties co-exist. With the passage of ARRA, for example, the healthcare sector encountered a scenario where entities were financially incentivized to adopt electronic medical records that met a particular standard, while failure to adopt had negative consequences on their reimbursement. Participants benefitted from doing the right thing, while contrarians incurred financial penalties for doing the opposite. The result, by 2021 96% of U.S. acute care hospitals complied with the adoption and utilization of certified electronic medical records.[159] While not a perfect outcome, addressing greater than 95% of any problem is generally viewed as a solid outcome.

Conversely, it is unlikely that a solution that offers solely a carrot or a stick would have a similar outcome. The passage of HIPAA in 1996, arguably the largest stick in the history of healthcare, has done little to change healthcare cybersecurity metrics since. In terms of volume, the trend toward the bad progressed nearly unabated following the implementation of HIPAA. A *HIPAA Journal* article stated, "our healthcare data breach statistics clearly show there has been an upward trend in data breaches over the past 14 years, with 2021 seeing more data breaches reported than any other year since records first started being published by OCR."[160] Most recently, a *Modern Healthcare* article

[159] Office of the National Coordinator for Health Information Technology, "Adoption of Electronic Health Records by Hospital Service Type 2019-2021," https://www.healthit.gov/data/quickstats/adoption-electronic-health-records-hospital-service-type-2019-2021.
[160] "Healthcare Data Breach Statistics," The HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/#:~:text=Between%202009%20and%202022%2C%205%2C150,population%20of%20the%20United%20States.

stated that "for 13 consecutive years healthcare data breaches have been the most expensive in any industry."[161] Since the HIPAA Privacy Rule compliance date in 2003, OCR received over 330,000 complaints, resolved over 320,000 cases, and levied more than $135,000,000 in fines.[162] These metrics ignore the nearly $38M per year taxpayers spend on enforcement at OCR, with the current administration putting forth a budget request to more than double that spend in 2024.[163] Yet, HIPAA did nothing to address the volume of attacks, nor the impact, all while levying fines and consuming massive amounts of private sector organizational resources to deal with security, privacy, legal, and regulatory compliance activities. The "stick" worked to no avail.

Similarly, it is unlikely that an incentives-only approach would work. According to one healthcare system chief executive "the incentives would have to be pretty significant to get my attention. The penalties embedded in HIPAA are more of a nuisance. If you were thinking about a construct that might work inside the board room of a large hospital system, you would need to consider something that has pretty significant incentives, otherwise my focus is going to be on other priorities like patient safety, clinical quality, better engaging our workforce, or trying to shore up our bottom line."[164] Allocating large sums of money in an altruistic fashion, in particular to the private sector, is unlikely to work. There would need be some form of construct, some framework for success, some reportable and verifiable means to assess and validate the

[161] Brock W. Turner, "Healthcare Data Breach Costs Keep Climbing: Report," *Modern Healthcare,* July 27, 2023, https://www.modernhealthcare.com/digital-health/data-breach-costs-hca-healthcare-hhs.
[162] A periodic update on CMS HIPAA enforcement efforts and metrics can be found at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html.
[163] U.S. Department of Health and Human Services, "Fiscal Year 2024 Budget In Brief," https://www.hhs.gov/sites/default/files/fy-2024-budget-in-brief.pdf.
[164] Anonymous Health System Chief Executive Officer, interview with Scott Blanchette, June 27, 2023.

intended outcomes, and some mechanism to ensure that achievements are sustained over time and not mothballed immediately thereafter. Achieving some modicum of success would prove valuable, sustaining that over time could provide immeasurable value.

Establishing a Gold Standard

Several systems and process certifications exist within the healthcare ecosystem today. Perhaps the most comprehensive is HITRUST. Established in 2007, HITRUST represents a collaboration between security experts, practitioners, policymakers, academics, and others who sought to create a healthcare-specific interpretation of several predecessor security policy frameworks. Most critically, The International Standards Organization ISO-27001, the National Institute of Science and Technology NIST 800-53, and several predecessor NIST and British Standard frameworks served as the foundation for the current HITRUST framework. This methodology is useful, requiring entities seeking certification to demonstrate the development and implementation of specific policies and procedures, and deployment and demonstration of those practices across an enterprise, and the continual training and evaluation of personnel to ensure compliance with those standards. Much like attestation letters developed by financial auditors, HITRUST certifications come with substantial qualifiers, including an acknowledgement that most of the technical controls that HITRUST seeks to regulate have not been tested, that there exist a universe of potential vulnerabilities that have not been assessed as part of the certification, and that management should not overstate the significance of HITRUST certification in practical, everyday operational terms. It is a start, but hardly an end.

Perhaps a role played by the ONCD, and the technical infrastructure it needs to assemble to better protect our nations critical assets, would be the continual technical assessment of the private sector. Much like a routine health check, the ONCD presumably would have the sort of both passive and active attack and penetration capabilities to engage broad swathes of the private sector, providing feedback on technical vulnerabilities exposed to the outside world. By engaging industry leaders who are adept at such activities and using artificial intelligence and machine learning to better target and focus assessment efforts, the ONCD could prove an invaluable resource in helping organizations risk mitigate vulnerabilities of which they are unaware.

Further, the ONCD should contemplate a code review process for private sector platforms of consequence. Like the Food and Drug Administration (FDA) approval for new drugs or the U.S. Department of Agriculture (USDA) approval for food products and production facilities, part of the ONCD mission statement could include certification for reviewed code that demonstrates secure coding practices, that eliminates potential software vulnerabilities pre-production, and ensures that key systems that run large swathes of our nation's critical infrastructure are built in the most resilient, reliable, and secure way possible. In healthcare, for example, three EHR's – Epic (35.9%), Oracle Cerner (24.9%), and Meditech (16.3%) represent more than 77% of the total market share.[165] It would not be unreasonable, nor impractical, for Epic, Cerner, and Meditech to be required to pass some code review process that eliminates many of the underlying vulnerabilities so commonly exploited in healthcare. To make matters even more

[165] Giles Bruce, "EHR Vendor Market Share in the US," Becker's Health IT, May 23, 2023, https://www.beckershospitalreview.com/ehrs/ehr-vendor-market-share-in-the-us.html.

promising, most of this code review is capable of being done absent the guidance of humans, using machines to isolate and identify problematic strings of code that would need to be remedied.

Conclusion

To say the U.S. has a long and difficult road ahead is a considerable understatement. We continue to expand our attack surface, underlie that surface with vulnerable and poorly secured platforms and processes, and are largely reliant on the expertise of individuals in short supply to key malicious actors at bay. Starting at the top, the U.S. needs a complete overhaul of how they prioritize, resource, and execute the nation's cyber strategy. Better, more accountable, executive leadership is a first step. Consolidating the redundant, poorly uniform, largely ineffectual cyber assets sprinkled throughout government represents a solid second step. Engaging in a partnership with entities capable of extending our threat picture and analysis capabilities over the horizon would further improve our nation's security posture. Employing offensive assets, where reasonable, would send the message to nations and criminals alike that cyber threats to our critical infrastructure will not be tolerated. Mobilizing and incentivizing the private sector will prove paramount in addressing the soft underbelly of America's cyber fabric.

The tools available in America's arsenal are near limitless. This not to suggest that every malicious cyber act demands a kinetic response. Quite the contrary. If every problem is viewed as a nail, every solution tends to look like a hammer. A binary, quid pro quo approach could prove highly problematic, and more importantly presents the prospect that cyber-conflict graduates to kinetic conflict. Professor Graham Allison

would argue that this sort of myopic cause-and-effect thinking is a classic representation of a move up the crisis ladder that inevitably leads to a catastrophic, kinetic conflict. As it relates to China and Russia, the U.S. must guard against the potential to graduate their responses beyond the point of return.

During the pandemic, America demonstrated a wide array of responses to counter the effects of the global pandemic, not the least of which was our willingness to print and distribute near-limitless amounts of money. While it remains a controversial response, and its long-term impact on American society remains to be seen, it demonstrates that America remains almost unconstrained in the array of solutions it can deploy in a crisis. Perhaps a construct to contemplate to address America's total lack of preparedness for a serious cyber-conflict might be something akin to the public works projects of the Great Depression Era. The relative degree of sophistication needed to run many of today's most advanced security assessment tools is quite low, at a time when America's tech literacy is at an all-time high. If we can find the money needed to pay people not to work for extensive periods of time, perhaps we can find the money to pay people to work on the myriad unaddressed areas that require shoring up across our critical infrastructure.

Failing to consider all the alternatives on the table leaves America not only vulnerable, but with a limited and highly problematic portfolio of responses to employ following a massive cyberattack on the U.S. critical infrastructure. It would be wise for America to recall the origins of the internet, spawned from the Defense Advanced Research Projects Agency, and remember that many of the notions that fueled investment and research into early computing and networking were national security related. For a full generation before broad commercialization, principles of national security guided our

thinking about the internet – protection, privacy, and enabling communications across known, secured, entities. Given the volume and nature of the threats the U.S. experienced during the COVID-19 pandemic, the destruction these attacks caused on a critically over-taxed healthcare system, and the culprits behind those attacks, perhaps it is time for the U.S. to revert to an orientation that more seriously addresses these threats and vulnerabilities, and does so before the nation finds itself – knowingly or not – on the doorstep of war.

Bibliography

Adler, Steve. "1.4 Million Individuals Affected by St. Joseph's / Candler Ransomware Attack." *The HIPAA Journal (*August 19, 2021). https://www.hipaajournal.com/1-4-million-individuals-st-josephs-candler-ransomware-attack/.

Adler-Milstein, Julia, Jay Holmgren, et al. "Electronic Health Record Adoption in US Hospitals: The Emergence of a Digital "Advanced Use" Divide." *Journal of the American Medical Informatics Association*, Volume 24, Issue 6 (November 2017): 1142–1148. https://doi.org/10.1093/jamia/ocx080.

Allison, Graham. *Destined for War: Can America and China Escape Thucydides's Trap?* Boston: First Mariner Books, 2017.

American Medical Association, "AMA Analysis Shows Most Physicians Work Outside of Private Practice," *AMA Press Release*, May 5, 2021. https://www.ama-assn.org/press-center/press-releases/ama-analysis-shows-most-physicians-work-outside-private-practice.

Anonymous Health System CEO, interview with Scott Blanchette, June 27, 2023.

Arntz, Peter, "Warning Issued About Vice Society Ransomware Targeting the Education Sector," *Malwarebytes*, September 7, 2022. https://www.malwarebytes.com/blog/news/2022/09/authorities-issue-warning-about-vice-society-ransomware-targeting-the-education-sector.

Barrett, Carter, "Eskenazi: Hospital Data Taken in Ransomware Attack," *NPR WYFI Indianapolis*, August 24, 2021. https://www.wfyi.org/news/articles/eskenazi-hospital-data-taken-in-ransomware-hack.

Barry, Ellen and Nicole Perlroth, "Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack," *New York Times*, November 26, 2020. https://www.nytimes.com/2020/11/26/us/hospital-cyber-attack.html.

Bernard, Rose, Gemma Bowsher, and Richard Sullivan, "Cyber Security and the Unexplored Threat to Global Health: A Call for Global Norms." *Global Security: Health, Science and Policy*, 5:1(2020): 134-141. https://doi.org/10.1080/23779497.2020.1865182.

Bodeen, Christopher, "Sign That Chinese Hackers Have Become Professional: They Take Weekends Off," *Huffington Post*, February 26, 2013. https://web.archive.org/web/20130226184036/http://www.huffingtonpost.com/2013/02/25/chinese-hackers_n_2756914.html.

Burgess, Matt, "The Workday Life of the World's Most Dangerous Ransomware Gang," *Wired.com*, March 16, 2022. https://www.wired.com/story/conti-leaks-ransomware-work-life/.

Center for Internet Security, "Breaking Down the BlackCat Ransomware Operation," *CIS Blog Posts.* https://www.cisecurity.org/insights/blog/breaking-down-the-blackcat-ransomware-operation.

Chalfont, Morgan and Maggie Miller, "Biden Administration Sanctions Russia for SolarWinds Attack, Election Interference," *The Hill*, April 15, 2021. https://thehill.com/homenews/administration/548367-biden-administration-unveils-sweeping-sanctions-on-russia/.

Chigada, Joel and Rujeko Madzinga. "Cyberattacks and Threats During COVID-19: A Systematic Literature Review." *South African Journal of Information Management* 23, no. 1 (February 2021). https://doi.org/10.4102/sajim.v23i1.1277.

Clarke, Richard A. and Robert K. Knake. *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. New York: Penguin Press, 2020.

Clausewitz, Carl von. *On War*, ed. Peter Paret, translated by Michael Eliot Howard. Princeton, NJ: Princeton University Press, 1989.

Congressional Research Service, "American Reinvestment Act of 2009 (P.L. 111-5): Summary and Legislative History," Washington, D.C. https://crsreports.congress.gov R40537.

Council of Economic Advisors, "The Cost of Malicious Cyber Activity to the U.S. Economy," February 2018. https://nsarchive.gwu.edu/media/17664/ocr.

Cozens, Bill, "5 Facts About Vice Society, The Ransomware Group Wreaking Havoc on the Education Sector," *MalwareBytes Labs Blog*, January 26, 2023. https://www.malwarebytes.com/blog/business/2023/01/5-facts-about-vice-society-the-ransomware-group-wreaking-havoc-on-k-12-schools.

Cyber Command P1AO, "Cyber 101 – U.S. Cyber Command Mission," October 18, 2022. https://www.cybercom.mil/Media/News/Article/3192016/cyber-101-us-cyber-command-mission/#:~:text=The%20mission%20of%20U.S.%20Cyber,spectrum%20of%20competition%20and%20conflict.

Cybersecurity and Infrastructure Security Agency, "Ransomware 101." https://www.cisa.gov/stopransomware/ransomware-101.

Cybersecurity and Infrastructure Security Agency, "China Threat Overview and Advisories." https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/china.

Cybersecurity and Infrastructure Security Agency, FBI, NSA, "Joint Cybersecurity Advisory: Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure," January 11, 2022. https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia.

Cybersecurity and Infrastructure Security Agency, "Ransomware Activity Targeting the Healthcare and Public Health Sector," October 28, 2020. https://www.cisa.gov/uscert/ncas/alerts/aa20-302a.

Cybersecurity and Infrastructure Security Agency, "#StopRansomWare: Vice Society," CISA Cybersecurity Advisory, September 8, 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-249a-0.

Cybersecurity and Infrastructure Security Agency, "Ransomware Activity Targeting the Health and Public Health Sector," CISA Cybersecurity Advisory, November 20, 2020. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-302a.

Cybersecurity Ventures, "Official Annual Cybercrime Report, 2019." https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report.

Dahukey, Aytan, Kenneth Yood, and Samuel O'Brien, "Venture Capital and Private Equity Investors Take Note: Primary Care May Become the Next Behavioral Health," *Lexology, Healthcare Law Blog*. August 5, 2020. https://www.lexology.com/library/detail.aspx?g=ef6ca53f-d115-4a57-a5e6-ace9baf7c2af.

Davis, Jessica, "10 Biggest Healthcare Data Breaches of 2021 Impact Over 22.6 M Patients," *SC Magazine*, December 21, 2021. https://www.scmagazine.com/feature/breach/10-biggest-healthcare-data-breaches-of-2021-impact-over-22-6m-patients.

Davis, Jessica, "Georgia St Joseph's/Candler Health System Shits to Downtime Procedures Amid Ransomware Attack," *SC Magazine*, June 22, 2021. https://www.scmagazine.com/news/malware/georgia-st-josephs-candler-health-system-shifts-to-downtime-procedures-amid-ransomware-attack.

Davis, Jessica, "Health Care a Culture of 'Yes': How EHR Modernization Raises Cybersecurity Challenges," *SC Magazine*, August 23, 2021. https://www.scmagazine.com/feature/risk-management/health-care-a-culture-of-yes-how-ehr-modernization-raises-cybersecurity-challenges.

Davis, Jessica, "Health Care Ransomware Attacks: Oklahoma Health System Driven to EMR Downtime," *SC Magazine*, June 16, 2021. https://www.scmagazine.com/news/malware/health-care-ransomware-attacks-oklahoma-health-system-driven-to-ehr-downtime.

Davis, Jessica, "UHS Ransomware Attack Cost $67M in Lost Revenue and Recovery Efforts," *Health IT Security*, March 1, 2021. https://healthitsecurity.com/news/uhs-ransomware-attack-cost-67-million-in-recovery-lost-revenue.

Deford, Drexel. "Sustainable Digital Health Demands Cyber Security Transformation," *National Library of Medicine, Front Health* 38, no. 3 (April 1, 2022): 31-38. https://doi.org/10.1097/HAP.0000000000000137.

Department of Treasury, "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," October 1, 2020. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

DiMaggio, Jon, "Ransom Mafia: Analysis of the World's First Ransomware Cartel," *Analyst1 Whitepaper*, April 7, 2021. https://analyst1.com/wp-content/uploads/2022/09/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLDS-FIRST-RANSOMWARE-CARTEL.pdf.

Fichtenkamm, Mark, Gerald Burch, and Jordan Burch. "Cybersecurity in a COVID-19 World: Insights on How Decisions are Made." *ISACA Journal*, Volume 2 (2022).

Fitzpatrick, Sarah and Kit Ramgopal, "Hackers Linked to Chinese Government Stole Millions in COVID Benefits, Secret Service Says," *NBCNews.Com*, December 5, 2022. https://www.nbcnews.com/tech/security/chinese-hackers-covid-fraud-millions-rcna59636.

Fokker, John, "Ryuk Ransomware Attack: Rush to Attribution Misses the Point," *Trellix Newsroom*, January 9, 2019. https://www.trellix.com/en-us/about/newsroom/stories/research/ryuk-ransomware-attack-rush-to-attribution-misses-the-point.html.

Government Accountability Office, "Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks," *Report to Congressional Committees*, June 2022, GAO-22-104256.

Greig, Jonathan, "White House Outlines Cyber Budget Priorities, Including Making Ransomware 'No Longer Profitable,'" *The Record Media*, June 28, 2023. https://therecord.media/white-house-cyber-budget-priorities-making-rasomware-not-profitable-zero-trust.

Healey, Jason. “The Spectrum of National Responsibility for Cyberattacks,” *The Brown Journal of World Affairs* 18, no. 1 (Fall/Winter 2011): 57–70. https://www.jstor.org/stable/24590776.

Health and Human Services, “HIPAA for Professionals.” https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.

Health and Human Services Office of Information Security, “HC3 Analyst Note,” *Report 202103231400*, March 23, 2021. https://www.cisa.gov/sites/default/files/publications/202103231400_Analyst_Note_CL0P_TLP_WHITE.pdf.

Health and Human Services Cybersecurity Program, “CLOP Poses Ongoing Risk to HPH Organizations,” *HC3 Analyst Note*, March 23, 2021. https://www.cisa.gov/sites/default/files/publications/202103231400_Analyst_Note_CL0P_TLP_WHITE.pdf.

Health and Human Services Office of the National Coordinator for Health Information Technology, “Adoption of Electronic Health Records by Hospital Service Type 2019-2021.” https://www.healthit.gov/data/quickstats/adoption-electronic-health-records-hospital-service-type-2019-2021.

Health and Human Services, “Fiscal Year 2024 Budget In Brief.” https://www.hhs.gov/sites/default/files/fy-2024-budget-in-brief.pdf.

Henry, JaWanna, et al, “Adoption of the Electronic Health Record Systems Among U.S. Non-Federal Acute Care Hospitals, 2008-2015,” *ONC Data Brief,* number 35 (May 2016). https://dashboard.healthit.gov/evaluations/data-briefs/non-federal-acute-care-hospital-ehr-adoption-2008-2015.php.

Herr, Trey, Steward Scott, and Maia Hamin, “The National Cybersecurity Strategy Implementation Plan: A CSI Markup,” *DFR Lab*, July 18, 2023. https://dfrlab.org/2023/07/18/national-cybersecurity-strategy-implementation-plan-markup/.

Hickey, Adam S., “Dangerous Partners: Big Tech and Beijing,” *US Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism*, March 4, 2020.

IBM, “Cost of a Data Breach Report, 2022.” https://www.ibm.com/downloads/cas/3R8N1DZJ.

IBM, "Cost of a Data Breach Report, 2020." https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf.

Institute for Security + Technology, "Combatting Ransomware: A Comprehensive Framework for Action, Key Recommendations from the Ransomware Task Force, 2021." https://securityandtechnology.org/wp-content/uploads/2021/06/IST-Ransomware-Task-Force-Report.pdf.

International Monetary Fund, https://www.imf.org/en/Publications/WEO.

Jacobs, Lee. "Interview with Lawrence Weed, MD- the Father of the Problem-Oriented Medical Record Looks Ahead." *The Permanente Journal* 13, no. 3 (2009): 84–89. https://doi.org/10.7812/tpp/09-068.

Jerich, Kat, "Cybersecurity Roundup: U.S. Agencies Warn of Russian Hacks, Australian Hospitals Struggle to Get Back Online," *Healthcare IT News*, April 27, 2021. https://www.healthcareitnews.com/news/cybersecurity-roundup-us-agencies-warn-russian-hacks-australian-hospitals-struggle-get-back.

Jerich, Kat, "Universal Health Services Faces $67M Loss After Cyberattack," *Healthcare IT News*, March 5, 2021. https://www.healthcareitnews.com/news/universal-health-services-faces-67-million-loss-after-cyberattack.

Khan, Navid Ali, Sarfraz Nawaz Brohi, and Noor Zaman, "Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic," *TechRxiv,* 2020. https://doi.org/10.36227/techrxiv.12278792.v1.

Kobus, Theodore and Craig Hoffman, "Baker Hostetler Launches 2023 Data Security Incident Response Report," April 27, 2023. https://www.bakerlaw.com/press/bakerhostetler-launches-2023-data-security-incident-response-report.

Krebs, Brian. "Ransomware, Data Breaches at Hospitals tied to Uptick in Fatal Heart Attacks," *KrebsOnSecurity*, November 7, 2019. https://krebsonsecurity.com/2019/11/study-ransomware-data-breaches-at-hospitals-tied-to-uptick- in-fatal-heart-attacks/.

Lallie, Harjinder Singh, Linsay Shepherd, et al. "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks During the Pandemic." *Computers & Security* 105, no. 102248 (2021). https://doi.org/10.1016/j.cose.2021.102248.

Landi, Heather, "UHS Breach Shows the Dangers Facing U.S. Hospitals With Growing Ransomware Threats," *Fierce Healthcare*, October 2, 2020.

https://www.fiercehealthcare.com/tech/uhs-breach-shows-dangers-facing-hospitals-growing-cyber-threats.

Lehmann, Christine, "Docs Refused to Pay the Cyber Attack Ransom – and Suffered," *Medscape*, January 5, 2022. https://www.medscape.com/viewarticle/966051.

Lovell, Daryl, "Medical Ransomware Attack Could Spell Disaster, Deaths During Pandemic," *Syracuse University STEM News*, September 29, 2020. https://news.syr.edu/blog/2020/09/29/medical-ransomware-attack-could-spell-disaster-deaths-during-pandemic/.

McDowell, Dagen, et al, "Warning To Russia: Biden To Confront Putin On Cyber Attacks And Election," *Mornings with Maria*, CQ Roll Call, June 22, 2021.

McKeon, Jill, "UVM Continues to Feel Effects of Ransomware Attack," *Health IT Security*, June 24, 2021. https://healthitsecurity.com/news/uvm-health-continues-to-feel-effects-of-ransomware-attack.

McKeon, Jill, "Conti Ransomware Group Continues to Threaten Healthcare," *Health IT Security*, March 10, 2022. https://healthitsecurity.com/news/conti-ransomware-group-continues-to-threaten-healthcare.

Moran, Greg and Paul Sisson, "Scripps Health Targeted by Cyberattack," *The San Diego Union Tribune*, May 2, 2021. https://www.sandiegouniontribune.com/breaking/story/2021-05-02/scripps-hospitals-it-by-it-security-incident-but-patient-care-go.

Morgan, Steve, "Cybercrime to Cost the World $8 Trillion Annually by 2023," *Cybercrime Magazine*, October 17, 2022. https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/.

Mosk, Matthew, "George W. Bush in 2005, 'If We Wait for a Pandemic to Appear It Will Be Too Late to Prepare,'" *ABC News*, April 5, 2020. https://abcnews.go.com/Politics/george-bush-2005-wait-pandemic-late-prepare/story?id=69979013.

Mucha, Michael, Interview with Scott Blanchette, June 23, 2023.

Newman, Lily Hay, "Russia's Sway Over Criminal Ransomware Gangs is Coming Into Focus," *Wired.com*, November 10, 2022. https://www.wired.com/story/russia-ransomware-gang-connections/.

Office of Civil Rights, US Department of Health and Human Services, "Breach Report Results." https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

Office of Civil Rights, US Department of Health and Human Services. "Covered Entities and Business Associates." HHS.gov, November 23, 2015. https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html./index.html.

Office of Civile Rights, US Department of Health and Human Services, CMS HIPAA enforcement efforts and metrics can be found at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html.

Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 6, 2023. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

Oladimeji, Saheed, and Sean Michael Kerner, "SolarWinds Hack Explained: Everything You Need to Know," *TechTarget*, June 27, 2023. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know.

Oliver, Michael, Andrew Pearce, et al. "The Impact of a Cyberattack at a Radiation Oncology Department: Immediate Response and Future Preparedness," *Advances in Radiation Oncology* 7, Issue 5, no. 100896 (September 2022). https://doi.org/10.1016/j.adro.2022.100896.

OnSecurity Team, "Ransomware: A Short History of Ryuk," *OnSecurity IO Blog*, November 16, 2020. https://www.onsecurity.io/blog/ransomware-a-short-history-of-ryuk/.

Page, Carly, "UK Battles Hacking Wave as Ransomware Gang Claims 'Biggest Ever' NHS Breach," *TechCrunch*, July 10, 2023. https://techcrunch.com/2023/07/10/uk-hacks-public-sector-nhs-ransomware/.

Patterson, Dan, "The World's Top Ransomware Gangs Have Created a Cybercrime 'Cartel'," *CBS News Money Watch*, July 22, 2021. https://www.cbsnews.com/news/ransomware-cybercrime-cartel-wizard-spider-viking-spider-lockbit-twisted-spider/.

PopulationU, https://www.populationu.com/gen/countries-by-gdp.

Poulson, Kevin, Robert McMillan, and Melanie Evans, "A Hospital Hit by Hackers, a Baby in Distress, and the First Alleged Ransomware Death," *Wall Street Journal*, September 30, 2021.

Relias Learning, "Cyberattack Almost Shuts Down Health System, Shows Need for Security," *Healthcare Risk Management* 43, no. 1 (2021).

Reveron, Derek S. and John E. Savage. “Cybersecurity Convergence: Digital Human and National Security.” *Foreign Policy Research Institute (*August 2020): 555-570. https://doi.org/10.1016/j.orbis.2020.08.005.

Rid, Thomas and Ben Buchanan. “Attributing Cyber Attacks,” *Journal of Strategic Studies*, 38:1-2 (2015): 4-37. https://doi.org/10.1080/01402390.2014.977382.

Schoen, Cath, Robin Osborn, et al. “A Survey of Primary Care Doctors in Ten Countries Shows Signs of Progress in Use of Health Information Technology, Less in Other Areas,” *Health Affairs*, Vol 31, No. 12 (December 2012): 2805 – 2016. https://doi.org/10.1377/hlthaff.2012.0884.

Scripps Health Overview found at https://www.scripps.org/about-us. Statistics dated June 28, 2023.

Seals, Tara, “Accellion Zero-Day FTA Attacks Show Ties to Clop Ransomware, FIN11,” *ThreatPost*, February 22, 2021. https://threatpost.com/accellion-zero-day-attacks-clop-ransomware-fin11/164150/.

Sentonas, Michael, “2020 Global Security Attitude Survey: How Organizations Fear Cyberattacks Will Impact Their Digital Transformation and Future Growth,” *CrowdStrike Blog*, November 17, 2020. https://www.crowdstrike.com/blog/global- security-attitude-survey-takeaways-2020.

Sherman, Justin, “Untangling the Russian Web: Spies, Proxies, and Spectrums of Russian Cyber Behavior,” *Atlantic Council, Cyber Statecraft Initiative, Issue Brief*, September 2022.

Sidorov, Jann. “It Ain't Necessarily So: The Electronic Health Record And The Unlikely Prospect Of Reducing Health Care Costs.” *Health Affairs* 25, no. 4 (July 2006):1079-85. https://doi.org/10.1377/hlthaff.25.4.1079.

Sophos, “Data Encryption from Ransomware Reaches Highest Level in Four Years Sophos’ Annual State of Ransomware Report Finds,” May, 2023. https://www.sophos.com/en-us/press/press-releases/2023/05/data-encryption-ransomware-reaches-highest-level-in-four-years.

Sophos, “Ransomware 2023,” May, 2023. https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf.

Soumerai, Stephen B. and Sumit R. Majumdar, “A Bad $50 Billion Bet.” *Washington Post*, Opinion. March 17, 2009.

Srinivasan, Suraj and Li-Kuan (Jason) Ni, "Ransomware Attack at Springhill Medical Center." *Harvard Business School Case* 123-065, February 2023.

Sweeney, John. *Killer in the Kremlin: The Explosive Account of Putin's Reign of Terror.* New York: Penguin Books, 2023.

Swivelsecure, "9 Reasons Healthcare Is the Biggest Target for Cyberattacks." https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/.

The HIPAA Journal, "Healthcare Data Breach Statistics," statistics dated June 6, 2023. https://www.hipaajournal.com/healthcare-data-breach-statistics/#:~:text=Between%202009%20and%202022%2C%205%2C150,population%20of%20the%20United%20States.

Tune, John, Lamar Alexander, Pat Roberts, Richard Burr, and Mike Enzi. "Where is HITECH's $35B Investment Going?" *Health Affairs Blog*, March 4, 2015. https://doi.org/10.1377/hblog201503045199.

Turner, Brock W, "Healthcare Data Breach Costs Keep Climbing: Report," *Modern Healthcare*, July 27, 2023. https://www.modernhealthcare.com/digital-health/data-breach-costs-hca-healthcare-hhs.

Umawing, Jovi, "Threat Spotlight: The Curious Case of Ryuk Ransomware," *Malwarebytes*, December 12, 2019. https://www.malwarebytes.com/blog/news/2019/12/threat-spotlight-the-curious-case-of-ryuk-ransomware.

Universal Health Services, Statement from Universal Health Services, October 29, 2020. https://bit.ly/2IoCLQp.

Universal Health Services, Investor Overview, June 28, 2023. https://ir.uhs.com.

U.S. CYBERSECURITY PREPAREDNESS AND H.R. 7331, THE NATIONAL CYBER DIRECTOR ACT, Hearing before the Committee on Oversight and Reform, House of Representatives, July 15, 2020.

Wachter, Robert M., MD, "Why Healthcare Tech is Still so Bad," *New York Times*, Sunday Opinion, March 21, 2015.

Wales, Brandon. "State and Local Cybersecurity: Defending our communities from cyber threats amid COVID-19," U.S. Senate Committee on Homeland Security and Government Affairs, Subcommittee on Federal Spending Oversight and Emergency Management, December 2, 2020.

Wall Street Journal - Cyber Daily Blog, "Trump Administration Says Russia Likely Behind SolarWinds Hack | Ransomware Attack Exposes Business, Personal Data at Peter Pan Seafoods." *WSJ Pro Online - Cyber Security*, 2021. https://www.wsj.com/articles/cyber-daily-trump-administration-says-russia-likely-behind-solarwinds-hack-ransomware-attack-exposes-business-personal-data-at-peter-pan-seafoods-11609940967.

White House Fact Sheet, "Imposing Costs for Harmful Foreign Activities by the Russian Government," April 15, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/.

White House PAO, "Office of the National Cyber Director," https://www.whitehouse.gov/oncd/.

White House, "Presidential Decision Directive – 63," May 22, 1998. https://irp.fas.org/offdocs/pdd/pdd-63.htm.

Witts, Joel, "Healthcare Cyber Attack Statistics 2022: 25 Alarming Data Breaches You Should Know," *Expert Insights*, March 28, 2023.

WTNH, News Channel 8, "Yale New Haven Health able to treat cancer patients again after nearly a week offline due to data breach," *News Channel 8 Online*, April 28, 2021. https://www.wtnh.com/news/connecticut/new-haven/yale-new-haven-health-confirms-its-among-over-40-health-systems-affected-by-cyber-security-breach/.

Yuceel, Huseyin Can, and Picus Labs, "Leaked Tools, TTP's, and IOC's by Conti Ransomware Group," *Picus Security*, March 4, 2022. https://www.picussecurity.com/resource/leaked-tools-ttps-and-iocs-used-by-conti-ransomware-group.

Zhadan, Anna, "Who Are Anonymous and Why Are They Fighting Alongside Ukraine," *CyberNews*, March 21, 2022. https://cybernews.com/editorial/who-are-anonymous-and-why-are-they-fighting-alongside-ukraine/.