THE HEALTHCARE RESEARCH SECURITY PANDEMIC

Threats to Patient Care, National Security, and the Economy

Authored By:
Drew Spaniel, Lead Researcher, ICIT
Parham Eftekhari, Founder & Chairman, ICIT
Executive Director, The Cybersecurity Collaborative

Contributors:
Dave Summit, CISO Moffitt Cancer Center and ICIT Fellow
Cris V. Ewell, CISO UW Medicine and ICIT Fellow

ICIT Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

MOFFITT CANCER CENTER®

The Healthcare Research Security Pandemic

Threats to Patient Care, National Security, and the Economy

May 2020

The authors would like to thank the following experts for their contributions to this paper:

- Dave Summitt, CISO Moffitt Cancer Center and ICIT Fellow
- Cris V. Ewell, CISO UW Medicine and ICIT Fellow

Contents

Introduction

The COVID-19 global pandemic is shining a spotlight on the critical role that the healthcare sector plays in national security, creating a unique opportunity to discuss the impact vulnerabilities have on this vital ecosystem. In the months since the outbreak of the virus, Chinese cyberespionage and advanced persistent threat (APT) attacks have spiked as adversaries targeted HHS and the wider medical sector in a broad campaign tailored to steal vital research. Malicious campaigns have posed as US agency officials in phishing emails, launched denial of service attacks, deployed ransomware, and spread disinformation. According to a senior Trump administration official, "The COVID-19 pandemic has provided a unique opening to nefarious actors and cybercriminals." The Director of the National Counterintelligence and Security Center, Bill Evanina, who has led the US intelligence community's battle against Chinese industrial and academic spying and theft of intellectual property, has also warned that critical research for Covid-19 vaccines risks being stolen and replicated overseas. In a CNN interview, Mr. Evanina commented, "Medical research organizations and those who work for them should be vigilant against threat actors seeking to steal intellectual property or other sensitive data related to America's response to the COVID19 pandemic." At a Strategic News Service event, John Demers, the head of the Justice Department's National Security Division, commented, "There is nothing more valuable today than biomedical research relating to vaccines for treatments for the coronavirus. It's of great importance not just from a commercial value, but whatever countries, company or research lab develops that vaccine first and is able to produce it is going to have a significant geopolitical success story."

> ***"Medical research organizations and those who work for them should be vigilant against threat actors seeking to steal intellectual property or other sensitive data related to America's response to the COVID19 pandemic."***
>
> *– William R. Evanina, Director of the National Counterintelligence and Security Center*

Meanwhile, a bipartisan group of senators, which included members of the Intelligence and Armed Services committees, urged Cyber Command and CISA to be more aggressive with their warnings and actions to ward off what they called an "unprecedented and perilous campaign of sophisticated hacking operations from state and criminal actors amid the coronavirus pandemic." Senators Tom Cotton, Richard Blumenthal, Mark Warner, David Perdue and Edward Markey wrote in a letter to NSA Director Paul Nakasone and CISA director Christopher Krebs that "Disinformation, disabled computers, and disrupted communications due to ransomware, denial of service attacks, and intrusions means critical lost time and diverted resources," and that "During this moment of national crisis, the cybersecurity and digital resilience of our healthcare, public health, and research sectors are literally matters of life-or-death [1]."

> ***"There is nothing more valuable today than biomedical research relating to vaccines for treatments for the coronavirus. It's of great importance not just from a commercial value, but whatever countries, company or research lab develops that vaccine first and is able to produce it is going to have a significant geopolitical success story."***
>
> *- John Demers, Assistant Attorney General of the National Security Division*

Today more than ever, millions of lives depend on the availability, accuracy, and integrity of healthcare networks as they treat patients, develop vaccines, and research medical solutions. During these aberrant times, another crisis looms over America's healthcare sector that threatens short and long-term public health, economic growth, and national security. Around the world, nation-state and criminal adversaries are aggressively exploiting vulnerabilities in healthcare research environments to steal intellectual property (IP) and disrupt medical device performance. These persistent attacks have led to billions of dollars in squandered research and development (R&D) resources, lost revenue, and ineffective care. Perhaps worst of all, these attacks have the potential to create inaccurate research conclusions that threaten one of the nation's most important economic drivers.

At the core of these attacks lies a war between nation-states predicated on great power competition and grounded in the theft of IP, the exploitation of stolen data, and, in some instances, the weaponization of key research that can be leveraged to harm an organization or nation. Pete Slade, ICIT Fellow and ThreatWarrior Founder and CEO, points out that "Healthcare research is a significant economic driver that creates new jobs, technologies, and products. Thus, cyberattacks that threaten to disrupt medical progress or lead to IP being stolen by nation-state actors compromise our economic stability and ability to globally compete."

"Healthcare research is a significant economic driver that creates new jobs, technologies, and products. Thus, cyberattacks that threaten to disrupt medical progress or lead to IP being stolen by nation-state actors compromise our economic stability and ability to globally compete."

- Pete Slade, Founder and CEO, ThreatWarrior

Attacks against the healthcare sector have proven lucrative in the past, and the sector as a whole remains vulnerable to disruptionware, Internet of Things (IoT) exploits, lateral compromise, insufficient cyber hygiene, and misaligned regulatory oversight. To mitigate these deficiencies, a holistic approach should be adopted that incorporates stakeholder needs and viewpoints, incentivizes security by design, holds device manufacturers accountable to security requirements, and trains all personnel to be cyber hygienic by default.

The healthcare sector depends on uninhibited innovation to fuel advancements in technology, improve patient care, and drive profits. If its leaders continue to eschew security and ignore the reality that their R&D is being targeted for theft, organizations will face insurmountable financial harm, our economy will suffer, our national security will degrade, and patients' lives will be lost. At a time when researchers are racing to create medical devices and treatments, it is more imperative than ever that the nation prioritizes the security of healthcare research environments.

Why is Healthcare Research Valuable?

Billions of dollars a year are spent on healthcare R&D, allowing America to benefit from being on the cutting edge of nascent technology and innovative treatments. Despite the value of the research to companies and their patients, healthcare research is often under-secured because:

- Healthcare stakeholders do not secure research according to its value
- Researchers lack awareness of threats and vulnerabilities
- Ensuring the Confidence, Integrity, and Availability of research assets are not priorities
- Many research environments rely on legacy systems or are secured by outdated paradigms, such as air-gap defenses

The combination of high-value research with a lack of effective security controls and training culminates in a complex threat landscape that so far has proven attractive, accessible, and lucrative for threat actors. Additionally, many healthcare research systems are integrated with clinical electronic records and data warehouses that may be subject to the security rules of the research applications instead of the layered controls of healthcare organizations. In short, research systems may become targets if they contain the same valuable data as other healthcare systems while being subject to fewer security controls.

One of the key findings of a December 2019 Research! America report was that R&D represents about 5% of healthcare spending, yet that amount was insufficient to meet the healthcare needs of the US population. Spending requests for cybersecurity to protect that research is even lower. They concluded, and the COVID-19 pandemic confirmed, that US R&D spending will need to drastically increase in the future [2].

2018 Medical and Health Stakeholder R&D Spending Exceeded $194.2 Billion		
	Percent of Annual Spending	**Spending**
Industry	66.7%	$129.5 Billion
Federal Government	22.2%	$43 Billion
Academic and Research Institutions	8.1%	$15.7 Billion
Foundations	1.2%	$2.3 Billion
State and Local Governments	1.1%	$2.1 Billion
Voluntary Health Associations and Professional Societies	0.8%	$1.5 Billion

While $194.2 billion is a staggering number, the true value of healthcare research is a combination of the capital investments made, the intellectual capital required to develop the IP, and the future value it brings to the organization and nation hosting said innovation. Only once a project is deemed ready-for-market, can organizations improve lives and drive revenue back to the organization that developed the technology. The US is already facing a historic shortage of healthcare professionals to care for its aging population, and competition is fierce for the technical talent required by healthcare R&D organizations. This limited pool of talent means domestic and global organizations have difficulties hiring and retaining the human capital needed to drive innovation.

This amalgamation of factors – capital required, go-to-market value, and human talent– is at the core of what makes healthcare research so valuable to nation-states and cybercriminals alike. Rather than overcome the obstacles required to develop healthcare IP, it is far easier to let someone else expend the time and resources then steal it for go-to-market exploitation.

How the Theft of Healthcare Research Damages our Nation

> ***"Rather than overcome the obstacles required to develop healthcare IP, it is far easier to let someone else expend the time and resources then steal it for go-to-market exploitation."***
>
> *- Drew Spaniel, Lead Researcher, ICIT*

The theft of healthcare research financially harms the victimized institution by denying it the ability to recuperate its R&D expenses and profit from its innovation. Disruptionware like ransomware can also have a significant impact on research environments by preventing access to data until the ransom is paid or the disruption removed. While security programs designed to protect redundancy and continuity of operations may reduce the threat of ransomware, there is no guarantee of data recovery or decryption by paying a ransom. Since ransomware variants are increasingly sold as a service, the bad actors who launched the attack may not have access to the decryption key. Decryption also does not guarantee the integrity of the files as they could be irreversibly damaged or modified in the process.

Other threats to the organization include the alteration of research data, which could mislead researchers and even harm patients during clinical trials. Research organizations that face a breach also face reputational damage, which could impact future funding, recruitment of top talent, and patient admissions. More nefarious outcomes include scenarios where medical research is weaponized by an adversarial threat actor. This could be realized by the development of chemical or biological weapons or a cyber kinetic attack through a vulnerability in a medical system or device.

It is also important to understand the harm these types of attacks present to national security. As mentioned above, the healthcare sector and its research are significant to the US economy; both are driven by innovation, which ultimately generates revenue from products and services. Nation-states such as China are systemically working to erode our nation's healthcare sector while boosting their own in an effort to replace the US on the global stage. The fastest path to accomplish this is to steal IP and directly or indirectly commoditize it with the ultimate goal of self-sustainment. China's strategy is based on long-term plans to establish independence from other countries and become the ultimate source of every major good and service.

This strategy is well documented and understood in the US intelligence community. China has already demonstrated its willingness to engage in economic espionage with recent high-profile crimes such as the theft of IP in order to develop the COMAC C919 airplane. According to an October 25, 2018 US indictment and a detailed report from CrowdStrike, China's Jiangsu State Security Division (JSSD) recruited or coerced at least ten insider threats at 13 western companies, most of them American, to steal sensitive aerospace research. The operation enabled COMAC to develop an aircraft comparable to those produced by Airbus and Boeing; however, thanks to saving billions of dollars and years of development resources, COMAC is able to offer the C919 cheaper than the U.S. competitors from which it stole research. This methodology is not unique to the aerospace sector. China's 14th Five-Year Plan dictates its prerogative to dominate all technological domains by 2025 [3] [4].

Another example is the Thousand Talents Program, established in 2008 by the central government of China and designed to recognize and recruit leading international experts in scientific research, innovation, and entrepreneurship. The US Senate Committee on Homeland Security and Governmental Affairs has identified it as a threat to US national security because the program requires participants to sign legally binding contracts with Chinese institutions. These contracts incentivize participants to lie on grant applications and steal intellectual property [5].

Chinese actors targeting healthcare research organizations have already been identified and apprehended by US law enforcement, and the Intelligence Community has recently issued a warning about this specific threat. In 2018, the FBI encouraged the NIH to send 18,000 letters urging health research administrators who oversaw government grants to be vigilant for insider threats and potential vectors for intellectual property theft. As a result, 71 institutions, including many of the most prestigious medical schools in America, are now investigating 180 individual cases involving the potential theft of intellectual property. At the time of writing, the NIH has referred 24 cases to the Office of Inspector General for the United States Department of Health and Human Services. In turn, these may become cases for criminal prosecution [6].

It is also important to consider the risk of vulnerabilities to the operational technology used in healthcare. As an example, the well-known Stuxnet malware targeted the programmable logic controllers that were used to automate the rotational speed of Iran's nuclear centrifuges. By altering the operational parameters of the centrifuges without alerting the operators, the attackers were able to stymie Iran's nuclear development. Similar equipment is the backbone of medical research and could be targeted by Stuxnet-like malware and other disruptionware to cause innumerable problems.

Who is Stealing Our Healthcare Intellectual Property?

Organizations involved in healthcare research and development – including treatments, medical devices, biotechnology, or other subsets of the industry - have valuable IP that is a driver for cybercriminals, economic espionage, and nation-state threats. Cybercriminals seek to exfiltrate personally identifiable information (PII) and protected health information (PHI); disruptive threats like ransomware hold irreplaceable systems, devices, and data sets hostage; and nation states carry out intrusions to steal valuable research and mass records for intelligence gathering purposes. For instance, China’s strategic “Made in China 2025” plan pushes for increased domestic development of medical technologies and devices, which may drive threat activity against IP holders and producers of these technologies [7].

FireEye also attributes a growing rise of healthcare research thefts by Chinese advanced persistent threats (APTs)to China’s concern over rising cancer rates, their lucrative domestic pharmaceutical market, and their pursuit of cost-effective universal healthcare. Targeting medical research and data from studies may enable Chinese corporations to bring new drugs to market faster than Western competitors, more rapidly develop innovative procedures, and capture geopolitical and market advantages in the global healthcare sector. According to Fire Eye, between 2018 and 2019 there were multiple attacks on research organizations from the Chinese-sponsored APT22, APT41, APT10, and APT18; Russian-sponsored APT28, APT29, and CyberBerkut; and the Vietnamese-sponsored APT32 [7].

Cyber threats on health care facilities can be divided into two categories: targeted and untargeted attacks [7]. Targeted attacks, often launched by insider threats or nation-state APTs, compromise strategic assets in order to achieve engineered outcomes. In contrast, untargeted attacks do not discriminate between assets and opportunistically compromise vulnerable devices. These are typically cybercriminal attacks motivated by short-term financial gains.

Independent Security Evaluators (ISE) identified the most likely adversaries faced by healthcare facilities. According to the report, "a small healthcare facility in an unpopulated area may not be concerned with nation-state or terrorist threats, while a metropolitan area hospital could be." Understanding the profile, motivation, and sophistication of adversaries is paramount to understanding the varying levels of threat actors, their capabilities, and their behavioral patterns [7]. The following high-level overview describes the most likely adversaries faced by healthcare facilities as well as their intentions regarding key assets:

- **Nation-state attackers** are the most likely to inflict long-term impacts on a healthcare research environment through sustained malware infections, the theft of valuable IP, the sabotage of research, and other targeted outcomes that the nation-state sponsor can leverage for economic or geopolitical capital. In some instances, such as the Chinese-sponsored Deep Panda attacks, an APT may target electronic health record databases to either facilitate future campaigns or for the operational insights that can be gleaned when datasets are subjected to machine-learning algorithms. These insights can lead to research, marketing, and other competitive advantages that can be realized on a global scale.
- **Criminal organizations** are motivated by immediate financial gain. Ransomware, the theft of sensitive research, or access-as-a-service operations are the most likely short-term impacts inflicted on healthcare research organizations by cybercriminals. In addition, because of the lack of efficient security controls in many healthcare organizations, the infection of an organization's network and assets makes it easy to launch distributed attacks on other locations via lateral compromises or botnets.
- **Other Threats Include:**
    - Insider threats are motivated by damaging the organization, stealing its research, or harming the public.
    - Cyberespionage actors sabotage research based on fiscal, ideological, or geopolitical motivations.
    - Individuals and small hacker collectives may be motivated by profit and notoriety.
    - Hacktivists are motivated by political and financial gain, most often seeking to embarrass, discredit, blackmail, or sell information about high profile individuals.
    - Terrorists are motivated by inspiring fear and causing harm.

Why are Research Environments Vulnerable to Attacks?

Like many technology sectors, a lack of security when designing devices and systems prevalent in healthcare research environments and poor cyber hygiene creates targets rich for exploitation. Significantly improving cybersecurity in healthcare research environments is not easy and will require cooperation from everyone, including doctors, nurses, IT professionals, and device manufacturers. The factors discussed below contribute to the vulnerability of healthcare research environments and can impact economic stability, organizational resiliency, patient outcomes, and national security.

Medical Devices are Not Designed for Integrated Environments

Much of the information technology (IT), IoT medical devices, and the operational technology (OT) running healthcare facilities, were not designed to interact with each other or with the security tools deployed on the network.

Medical devices are often developed in research environments without comprehensive security. They are presumed to operate in isolation when, in fact, many of these "isolated" devices are outdated or are networked with other internet-enabled devices. Further, network isolation is not a sufficient replacement for security by design. Many "isolated" devices are networked to internet-enabled systems, are updated from flash drives that are plugged into Internet-enabled systems or are accessible by potential insider threats. These technologies are often vulnerable to cyberattacks, which can siphon off data, hijack processing for cryptocurrency mining, or shut down an entire hospital until a ransom is paid.

Non-Medical, Internet of Things Devices can be Exploited

Research environments are also threatened by non-medical, IoT devices such as IoT sensors used to track medical equipment, building automation, network components, and staff wearables. Irresponsible software development and device engineering practices plague IoT manufacturers who value functionality, speed-to-market, and cost over security. When these devices are brought into the research environment and connected to a network, they can act as beachheads for adversaries who exploit their vulnerabilities to gain access and move laterally across the network [8].

The rise in bring-your-own-device policies and wearable technologies further adds to the growing IoT landscape within research organizations, including mobile phones, tablets, and smartwatches. If these devices are infected with malware, adversaries could leverage them to laterally compromise any sensitive research networks to which they connect.

Insider Threats

Despite repeated warnings from experts, including intelligence agencies like the National Counterintelligence & Security Center, insider threats continue to be a significant threat to the research community. Insider threats can be organized into two categories:

- **Non-malicious insider threats** are personnel who unintentionally expose the organization to risk or compromise. This can include undertrained staff who fall victim to phishing attacks, negligent workers who ignore training and best practices, mismanaged third-party contractors whose credentials are compromised or have poor cyber-hygiene practices, and overwhelmed personnel who inadvertently expose the organization to malware despite their good intentions. In research environments, there may be less focus on data security or access controls, especially if the controls are perceived as a barrier to research. In some cases, external researchers, such as collaborators or affiliated third parties, may have access to sensitive data. Unenforced access controls could lead to non-workforce members inappropriately accessing clinical data, opening the door to third-party attacks from outside the organization and creating the opportunity for lateral compromise.
- **Malicious insider threats** are individuals from the primary organization who intentionally steal data, compromise security, or otherwise harm their employer. There are several types of insider threats, including disgruntled employees, departing executives who promise their new employers IP, and nation state-sponsored threats working on behalf of an adversary. Malicious insider threats can be recruited after hiring or planted within a target organization, adding an additional layer of complexity to this category of threats. These threats are the most challenging to defend against, which is why China’s Thousand Talents Program works.

The Convergence Between Information and Operational Technology

The increasing reliance on the internet and network-connected OT in research environments has significantly expanded the threat landscape. Building automation, electrical infrastructure, and fire and safety systems with poor security are often overlooked, yet these systems can serve as entry points for adversarial campaigns.

The damage done from the exploitation of OT vulnerabilities can have numerous dangerous outcomes. The breach of a research organization's network could give hackers access not only to critical infrastructure functions such as water or electricity, but high computing power clusters. Many of these clusters are powerful enough that they have controlled access regulated by the federal government. Attacks to the power, HVAC, or water systems could inhibit the proper temperature control of vital research samples. In many cases, the potential of the attack is limited only by the imagination of the attacker and the vulnerability of the support system.

How Can We Defend our Healthcare Research?

Stakeholders must act quickly to secure IP, sensitive data sets, and medical devices against adversaries who are intent on jeopardizing patient health, damaging the national economy, and threatening national security. Research organizations must hold vendors to higher security standards and educate business leaders on the long-term risks to the organizations if the threats are not mitigated. An approach similar to how the U.S. Department of Defense is incentivizing the Defense Industrial Base to improve security through the CMMC initiative is advised. Some of ICIT's recommended areas of focus are detailed below.

Increase Manufacturer, Security, and Research Community Communities

Cybersecurity is most effective when stakeholders operate in concert to develop secure systems and devices that meet the needs of the user. Device manufacturers and software developers must increase their engagement with cybersecurity and healthcare research leaders during the engineering and design process to improve technology resiliency. This information exchange should aim at improving security by focusing on:

- Supply chain security for applications, medical devices, IoT devices, and operational technology
- The prioritization of security-by-design, penetration testing, and development security operations (DevSecOps) during the development lifecycle
- The development and testing of devices testing in interconnected, real environments as opposed to isolation

Improve Cyber Hygiene Training for All Personnel

Threats such as ransomware, compromised credentials, and data leakage are often the result of undertrained personnel falling victim to phishing attacks, missing signs of insider threat activity, or other poor cyber-hygiene practices. Healthcare research environments must ensure that cybersecurity awareness is a core value for personnel by:

- Conducting regular cybersecurity awareness training for all personnel
- Asking Leadership to lead by example and follow the same security protocols as non-executives
- Establishing phishing awareness campaigns

Cybersecurity awareness will also organically increase if more researchers and non-cyber personnel become involved in the manufacturing and development process as they will better understand the risks of insecurity. There is also a need for enhanced, required researcher training focused on data use. Many researchers lack understanding of the limitations of IRB approval and their responsibilities. They broadly misunderstand the limitations of IRB approval and of the state-mandated Confidentiality Agreements or they perceive IRB approval and the Confidentiality Agreements as the only necessary requirements for accessing records (including PHI) and for entering facilities to conduct research.

Implement an Integrated Security Strategy

Healthcare research organizations must develop and implement integrated security to defend their networks, systems, and devices from adversarial compromise. This strategy should be built around the confidentiality, integrity, and availability of systems and data. Some specific efforts include:

- Creating a dedicated information security team
- Conducting regular cybersecurity and vulnerability assessments
- Training every employee on cybersecurity awareness
- Leveraging frameworks and commonly accepted security models such as zero-trust methodologies and the NIST Cybersecurity Risk Management Framework
- Ensuring critical data are segmented and redundancies and backups are in place to minimize the effect of a disruptionware attack
- Implementing policies and procedures to manage employee and contractor access to data
- Implementing principles of least access, including turning off access for former personnel
- Developing policies to address non-compliant personnel and contractors
- Standardizing data protection controls across departments and monitoring for unauthorized access, use, or disclosure of clinical data
- Reporting clinical data breaches and disclosing potential security issues to the covered entity
- Including security, data management, and enhanced training requirements in data use and business associate agreements
- Evaluating lower risk alternative approaches to data sharing
- Requiring a data use agreement which allows cybersecurity personnel to review the arrangements for all shared research data, including all forms of clinical data

Clearly Identify the Clinical Data Requiring Oversight

The categorization of clinical data according to its sensitivity can help protect data according to its value and potential to inflict harm if stolen. Oversight helps address gaps with respect to stewardship of PHI and other forms of sensitive clinical data, including de-identified data. Efforts should remove any ambiguity regarding stakeholder obligations to protect PHI whether it is shared, remains within organizations, or is removed from the covered entity such as when clinical data is stored in an electronic file in a researcher's offsite office. Additionally, metrics should be created to clarify when research data should be considered PHI based on its necessity and sensitivity. Furthermore, categorization guidelines should dictate when removing data requires authorization, who is responsible for tracking the data, and how to account for disclosures.

Update Regulatory Frameworks

The Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) focus on the security of patient's PII and on patient environments but fail to adequately ensure comprehensive security in healthcare research environments. The frameworks are also at risk of becoming outdated due to the rapid development of technology and the acceleration of sophisticated threats. To ensure that security in healthcare research environments is properly regulated, ICIT recommends:

- Updating frameworks to reflect the risk posed to modern healthcare research environments, accounting for different organization types
- Phasing out and blocking devices that were developed without built-in security or that are known to be vulnerable
- Updating the Food and Drug Administration's (FDA's) certification requirements to include security provisions for the lifecycle management of devices, potentially requiring more than minimal compliance regulation or a focus on incentives to improve behaviors rather than penalties for non-compliance

Resources for Healthcare Research Community Resiliency

The healthcare research community can leverage the following resources to support its security operations and improve resiliency:

- The American Hospital Association (AHA) encourages its members to invest in cybersecurity and has proposed many plans to help them do so
- The HITRUST initiative offers a monthly cyber threat briefing about the latest news and best defense practices while helping companies identify early warning indicators of compromise
- The Health Information Sharing and Analysis Center (H-ISAC) provides a proactive stance on cybersecurity, raising awareness among healthcare actors, providing security standards and protection policies, and assessing global cyber risks
- The FDA coordinates both manufacturers and users of medical devices to improve resiliency and patient safety

Time is Running Out to Secure Healthcare Research

The disruption caused by the global COVID-19 pandemic underscores the importance of healthcare research to global stability. Manufacturers and research organizations should prioritize cybersecurity throughout the product lifecycle, and research environments should feature integrated security wherever data is stored, processed, or transported. The time has come for the healthcare community to place an appropriate focus on defending healthcare research from adversaries to protect individual health, organizational resiliency economic stability, and national security.

Sources

[1] Z. Cohen and A. Marquardt, "'They are trying to steal everything.' US coronavirus response hit by foreign hackers", CNN, 2020. [Online]. Available: https://www.cnn.com/2020/04/25/politics/us-china-cyberattacks-coronavirus-research/index.html. [Accessed: 29- Apr- 2020].

[2] J. Lagasse, "Investment in medical and health R&D not keeping up with needs of nation, report finds", Healthcare Finance News, 2020. [Online]. Available: https://www.healthcarefinancenews.com/news/investment-medical-and-health-rd-not-keeping-needs-nation-report-finds. [Accessed: 01- Apr- 2020].

[3] J. Ferry, "How China Stole an Entire Airplane", *IndustryWeek*, 2019. [Online]. Available: https://www.industryweek.com/the-economy/article/21118569/how-china-stole-an-entire-airplane. [Accessed: 09- Jan- 2020].

[4] R. Hackett, "Chinese Hacking: The Plane Made from Stolen Tech?—Cyber Saturday", *Fortune*, 2019. [Online]. Available: https://fortune.com/2019/10/19/chinese-hacking-plane-stolen-tech-cyber-saturday/. [Accessed: 09- Jan- 2020].

[5] "Securing the U.S. Research Enterprise from China's Talent Recruitment Plans", *Hsgac.senate.gov*, 2019. [Online]. Available: https://www.hsgac.senate.gov/subcommittees/investigations/hearings/securing-the-us-research-enterprise-from-chinas-talent-recruitment-plans. [Accessed: 09- Jan- 2020].

[6] G. Kolata, "Vast Dragnet Targets Theft of Biomedical Secrets for China", *Nytimes.com*, 2019. [Online]. Available: https://www.nytimes.com/2019/11/04/health/china-nih-scientists.html. [Accessed: 09- Jan- 2020].

[7] Beyond Compliance: Cyber Threats and Healthcare", FireEye, 2020. [Online]. Available: https://content.fireeye.com/cyber-security-for-healthcare/rpt-beyond-compliance-cyber-threats-and-healthcare. [Accessed: 17- Apr- 2020].

[8] "IoT in Healthcare Industry | IoT Applications in Healthcare - Wipro", *Wipro.com*, 2018. [Online]. Available: https://www.wipro.com/en-IN/business-process/what-can-iot-do-for-healthcare-/. [Accessed: 09- Jan- 2020].