CHIME DIGITAL HEALTH LEADERS

Written Testimony of Scott MacLean
CHIME Board Chair and SVP and CIO of MedStar Health
House Energy and Commerce Subcommittee on Health
"Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack"
Tuesday, April 16, 2024

Good morning, Chairman Guthrie, Vice Chair Bucshon, Ranking Member Eshoo and members of the Subcommittee. My name is Scott MacLean, and I am the Board Chair for the College of Healthcare Information Management Executives (CHIME) and Senior Vice President (SVP) and Chief Information Officer (CIO) of MedStar Health. With over 25 years of experience in Health Information Technology (HIT), I am grateful for the opportunity to represent CHIME's membership in today's hearing focused on "Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack."

CHIME is an executive organization dedicated to serving over 5,000 CIOs and other senior healthcare IT leaders in diverse healthcare settings nationwide, as well as worldwide. Our members represent provider organizations of varying sizes, including large hospital systems, community hospitals, for-profit hospitals, small or rural hospitals, long-term care facilities, and critical access hospitals. CHIME members are among the nation's foremost health IT experts, including on the topics of cybersecurity, privacy and security.

We appreciate the Subcommittee convening this hearing on the unprecedented cyberattack on Change Healthcare, a unit of UnitedHealth Group (UHG), given the ongoing impacts faced by our members. Before addressing these impacts, we would like to express our gratitude to the Subcommittee for its continued attention to improving the cyber posture of the Healthcare and Public Health (HPH) Sector, one of the 16 critical infrastructure sectors in the U.S.

We applaud lawmakers for passing the Protecting and Transforming Cyber Health Care Act of 2022 (PATCH Act), included in the 2023 Consolidated Appropriations Act,[1] which gave the Food and Drug Administration (FDA) greater oversight authority over medical device cybersecurity. Additionally, P.L. 116-321[2] which incentivized Health Insurance Portability and Accountability Act

[1] H.R.2617 - 117th Congress (2021-2022): Consolidated Appropriations Act, 2023 | Congress.gov | Library of Congress
[2] PUBL321.PS (congress.gov)

(HIPAA) covered entities to align their cybersecurity best practices to Section 405(d) of the Cybersecurity Act of 2015, was strongly supported by CHIME.

We have made significant progress advancing the posture of our sector over the past several years, but we know we have a lot of work ahead of us and this will require robust federal support.

<u>Overview of Healthcare Cybersecurity Landscape</u>:

Hostile nation states have grown increasingly aggressive with their tactics, attacking hospitals and other healthcare stakeholders daily. This poses an imminent risk to our national defense. Bringing down a hospital or multiple healthcare delivery organizations (HDOs) at once is a risk for the nation and it shakes the confidence and trust of everyday Americans which is precisely what hostile nation states intend. They are looking to exact both physical, financial, and psychological harm.

Healthcare data and patient information remain lucrative targets for theft and exploitation, particularly through ransomware attacks. Criminal groups and adversarial nation states utilize tactics, techniques and procedures across our Sector – including large, publicly traded companies with far greater resources than most U.S. hospitals and health systems.

The costs to recover from a data breach in the HPH Sector are staggering – averaging $10 million per incident, which is far higher than any other sector. As a comparison, the costs for a financial entity to recover from a breach are estimated to be $6 million.[3] The fallout after an attack has also been shown to impact patient care – one report found that nearly a quarter of organizations suffering a cyber breach experience higher patient mortality rates.[4] In short, cybersecurity is now also patient safety.

Our members are committed to adopting cybersecurity best practices and take their responsibility to protect not only the privacy and security of patient data and devices networked to their system – but critically – their patient's overall safety and well-being very seriously. Currently, hospitals are forced to balance the challenges of the high cost of cyber insurance, near-constant cyberattack attempts, the inherent risks to their patients, the weaponization of artificial intelligence (AI), and the current workforce shortage needed to mitigate all these risks. They are doing their best to navigate an ever increasingly complex cybersecurity landscape, a

[3] IBM report finds that cybersecurity attacks impact healthcare more than any other sector | Modern Healthcare
[4] pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf (proofpoint.com)

job that has become infinitely more complicated with managing third-party risk as vendor/supporting parties are unwilling to sign HIPAA business associate agreements (BAAs), and/or are resisting acceptance of appropriate levels of liability recognizing the great amounts of protected health information (PHI) they maintain/process. Hospitals nonetheless undertake and devote significant resources to securing their systems because they are truly committed to the health, well-being, and safety of patients in the communities they serve.

Like nearly all organizations in the United States, hospitals and HDOs must care – to some degree – about their ability to generate positive net revenue in order to keep their doors open. However, they are unlike other organizations in that their first and most important mission is to care for their patients. Hospitals and healthcare systems are not only critical to the communities in which they serve, they are also often the largest employers.

We must continue to move away from a mentality that punishes those that have been victimized by malicious actors and criminals. Cybersecurity is a shared responsibility across the community of hospitals and health care systems – as well as supporting third-party vendors and affiliated continuum of care providers; however, without additional assistance, the Sector is limited in what we can do.

Impact of Change Healthcare Cyber Incident:

On February 21, 2024, Change Healthcare discovered a threat actor gained access to one of their environments. A Russia-affiliated ransomware group known as ALPHV/BlackCat has claimed responsibility. This is the most massive cyberattack on our sector to date – much larger than the WannaCry event experienced several years ago – and it has wreaked unprecedented havoc on the entire healthcare ecosystem given the data clearinghouse and transaction hub role that Change provides at national scale. It has and continues to interrupt patient care and the financial impact on our members has been devastating. Further, they are still ongoing, and have not been fully resolved. This incident has been likened to the “Colonial Pipeline” of healthcare, highlighting the scale of Change Healthcare's impact with 15 billion healthcare transactions processed annually and touching one in three patient records.[5]

Following the attack, there was a dearth of information and our members found themselves in the dark navigating an extremely complex and far-reaching attack with few answers, and few

[5] Letter to Health Care Leaders on Cyberattack on Change Healthcare | HHS.gov

options for continuing operations. The lack of answers hampered and continues to hamper recovery efforts. Many of our members were not invited and/or were unaware of the weekly calls hosted by UHG sharing updates on mitigation efforts. Indicators of compromise (IOCs) were not widely shared immediately, third-party attestations as to which systems were "safe" to reconnect to were not immediately available, questions about whether data was exfiltrated by the criminals has yet to be confirmed, and a list of payers with direct connections to Change was only made available several weeks after the cyber incident occurred. From the very beginning there was significant confusion about where to turn for help and our members found themselves struggling to navigate the most significant cyber incident to hit our sector.

Recognizing the need for greater transparency and assistance, CHIME reached out to the U.S. Department of Health & Human Services (HHS), the Centers for Medicare & Medicaid Services (CMS), the Administration for Strategic Preparedness and Response (ASPR), and colleagues at other provider organizations to navigate this incident, establish workarounds and stem the spread of this attack. On March 1st we shared several examples of the impact on patient care, providers, and other stakeholders with the Administration. These included patients being unable to get their prescriptions filled, being forced to pay out-of-pocket prices, patients with complex conditions and costly medications like chemotherapy therapy treatments searching for a way to pay for their medications, and the inability of patients to use medication coupons.

HHS' ASPR acts as the Sector Risk Management Agency (SMRA) for cybersecurity incidents pursuant to Section 9002 of the National Defense Authorization Act of 2021. On March 5, HHS issued a press statement acknowledging the incident, two weeks following the attack. This is in stark contrast to the way ASPR handled the WannaCry attack in 2017 when calls to share details began nearly immediately by the Administration to impacted stakeholders. Without a clear sense of where to turn, recovery efforts from the inception of this attack were hampered.

In an effort to assist our members, CHIME submitted a letter to HHS Secretary Xavier Becerra on March 26th outlining some of our member's continued concerns, including the insufficient level of detail shared by UHG and requesting more outreach to providers.

As we near the point of eight weeks since the initial cyberattack on Change, the fallout and financial impact stemming from this cyberattack continues to impact not only our members – but the entire healthcare ecosystem. A subset of the cyber criminals is rumored to have issued a second ransom demand fueling more questions and stoking fear among those who have yet to reconnect whether it is safe to do so. What once was a trusted network, can no longer be trusted and industry trust will not be established until transparency is used to address specifics of the exploit, details are shared of the recovery efforts taken to date, as well as additional mitigating controls that have been put in place.

The Change Healthcare attack has laid bare how interconnected our healthcare system is and the only way to defeat the enemy is to work together. This sentiment is shared by former National Cyber Director Chris Inglis who has said, “we have to establish this critical infrastructure partnership construct (i.e., The Health Sector Coordinating Council) in such a way that you have to beat all of us to beat one of us.”[6] In a recent Congressional briefing we hosted, our members shared similar thoughts.[7] It has also highlighted the impact of vertical integration of our sector which continues to spawn large mergers and acquisitions.

Once the magnitude of the attack became clear, the impacts to cash flow were severe and many providers still have not recovered. The cash flow impact has been especially pronounced for small and under-resourced providers. Many of our members have had to divert staff resources to implement workarounds needed to continue business operations and receive reimbursement.

Survey Results

In preparation for this hearing, CHIME polled our membership in a small survey to better understand the ongoing impact of the Change Healthcare cyberattack. The results are disheartening even for those of us who have been active in the cybersecurity landscape for years, and with healthcare being under constant threat.

When asked, “**Have you opened up/connected back to any Change Healthcare services yet?,**” 54 percent of members surveyed responded that have reconnected to some Change Healthcare services, 21 percent have not reconnected any services, 13 percent have reconnected to all services, and 12 percent did not have any directly connected services.

When assessing the **priority areas for federal support needed** to improve healthcare providers’ cyber posture, our survey results highlight a diverse range of critical areas. The question was: “If the federal government were to offer support to healthcare providers to

[6] A Conversation with Chris Inglis and Anne Neuberger (csis.org)
[7] Key-Takeaways-on-Cyber-Briefing-FINAL__1_.pdf (ctfassets.net)

improve their cyber posture – which areas would be priorities (or most impactful) for you/your organization?" Respondents could only select their top three from the twelve options.

1. **Mandating Payers and Third-Parties Compliance:**
   - 50 percent of respondents emphasized the need to enforce cyber best practices across payers and other third-parties (e.g., Cloud Service Providers), aligning with the aforementioned 405(d) Program.
2. **Financial Assistance and Incentives:**
   - 46 percent recognized the significance of financial support in the form of incentives or other payments to bolster cybersecurity efforts.
3. **Emergency Designation and Safe Harbors for Threat Information Sharing:**
   - 38 percent advocated for designating major cyber incidents in healthcare as a national emergency, thereby unlocking additional federal resources.
   - Simultaneously, 37 percent sought additional "safe harbors" for sharing threat information during cyber incidents and a catastrophic federal cyber insurance program/offering.

Furthermore, 23 percent of members expressed interest in the **Office for Civil Rights (OCR) offering relief/alternatives related to breach notification requirements**. These findings underscore the multifaceted approach needed to safeguard the healthcare ecosystem against cyber threats.

In assessing the impact of the Change cyber incident on patient care, the survey results reveal a nuanced yet concerning picture. We asked our members, "**On a scale of 1-5, how much of an impact did the Change cyber incident have on any patient care**?"

- 40 percent of respondents reported a somewhat impacted effect.
- 25 percent indicated a moderate impact.
- 15 percent stated a very significant impact.
- Fortunately, 13 percent claimed no impact.
- A smaller, but notable 5 percent faced an extremely impactful situation to patient care.

These responses underscore the complex consequences of the incident, ranging from minor disruptions to critical delays and impact on patient care. Because patient care is at the heart of each of our members' core mission, even one member reporting that this incident impacted patient care is unacceptable.

The responses also are reflective of the core nature of healthcare. Care delivery and business continuity strategies are already in place to address unplanned downtimes, as manual processes are relied upon to ensure delivery of quality patient care during a technology disruption. While care will be the primary focus, the operational ability to determine eligibility, schedule procedures, deliver medications, submit claims, and receive payments is what is hampering and financially impacting the industry.

In response to our query regarding **the mandatory implementation of the 20 HHS Cybersecurity Performance Goals (HHS-CPGs) and our members' ability to comply without federal financial assistance**, our survey results revealed that 40 percent are unsure (i.e., selected "Maybe"), 33 percent said that they would be able to, and 27 percent said candidly and firmly, "No." These diverse viewpoints underscore the complexity of achieving compliance with the CPGs without federal financial assistance. We respectfully request that Congress navigate these policies carefully, ***with*** hospitals, health systems, clinics, and practices – to enhance their cybersecurity posture and safeguard patient care and patient data.

The Change Healthcare cyber incident has had far-reaching and severe consequences for hospitals and health care systems. **CHIME's member survey results demonstrate that a substantial majority of members – 85 percent – experienced detrimental impacts on their claims, while 81 percent suffered setbacks in reimbursement. Additionally, 75 percent grappled with disruptions to their revenue cycle, and 71 percent encountered issues with claims submission (either all or partial).**

The repercussions extended to pharmacy services, affecting 58 percent of respondents, and prior authorization services, impacting 52 percent. Even the service option with the least impact, care management, still affected 15 percent of our members. Beyond these core services, other critical functions such as pharmacy coupon services, denial of claims, interoperability, and radiology image sharing were also adversely affected. **These findings underscore the ongoing need for detailed information and updates from UHG and the financial assistance that is still needed to safeguard patient care, ensure financial stability, and restore operational continuity across the healthcare ecosystem.**

As part of our survey, we were also able to capture first-hand testimonials from providers describing current and ongoing challenges:

- “The preparation of healthcare providers is only as good as the connections they have to others. That may be vendors, other providers, other healthcare related entities. If there is a weak link in the chain, then we are all at risk and need to know how to plan together as a whole.”
- “I would also recommend minimum cyber standards for ALL third-party providers providing ANY services to healthcare. This includes business applications and clinical (EMR, medical devices, etc.) We are defining the scope of "healthcare" too narrowly causing holes in our defenses - leading to events like Change Healthcare.”
- “Change Healthcare is a large entity and we’re still impacted. Small rural hospitals do not stand a chance against threat actors because of financial reasons.”
- “We don't have the resources or funds to meet all the cyber demands. Labor costs and supply chain issues along with inflation are preventing our recovery to pre-pandemic revenues. But even then, there were minimal dollars we could spend as a small to medium sized hospital.”

Patient safety in the healthcare sector means not just ensuring access to care but ensuring that patient safety is not jeopardized. Change Healthcare has not provided any detailed reporting of all the vulnerabilities exploited during this cyberattack – and we believe that their reputational protection and legal liability positioning should not be prioritized over patient safety and the overall operational health of the nationally connected healthcare industry. This lack of transparency has hindered our collective recovery efforts, made it more costly, lengthier, and diverted precious provider resources away from other critical functions. It has also continued to cause downstream impacts such as larger payors and/or clearinghouses either not reconnecting or being slow to do so thus keeping critical funding away from the healthcare delivery organizations and providers that need it the most.

Cybersecurity must be a joint responsibility across stakeholders throughout the entire ecosystem of healthcare – not simply a subset. Otherwise, it inadvertently shifts more burden onto providers, many of which are already severely strained, understaffed, and under-resourced all while providing quality patient care. In the ongoing battle against cyber threats, we cannot over-emphasize the need for a united and concerted front, recognizing that cybersecurity is a shared responsibility.

While providers may not be able to completely avoid every cybersecurity incident – especially when they are not the ones directly experiencing the attack – steps taken to decrease the timeline between the discovery of the threat and mitigation of the threat is critically essential to increasing patient safety and restoring healthy operations. The healthcare adage "time is brain" applies here as well, recognizing that more timely, quicker care results in better outcomes. The technology parallel is "time is containment" with the result being reduced impact to operations and better operational and financial outcomes.

Summary of Policy Recommendations:

Below, you will find a comprehensive summary of our policy recommendations, designed to address the challenges discussed and to guide future legislative action in Congress.

General Funding

With the healthcare sector only as strong as its weakest link, it is imperative that the federal government prioritize programs designated to aid small and under resourced HDOs protect themselves against, detect, respond to, or recover from cybersecurity threats. These programs can be successful by providing funding or technical assistance to help eligible HDOs adopt recognized cybersecurity practices – such as the 405(d) Program, recognized by Congress in P.L.116-321 – to replace legacy systems and devices, conduct security risk assessments, generate corrective action plans for mitigating identified risks, or hire staff.[8]

Funding to Implement Cyber Performance Goals (CPGs)

CHIME is supportive[9] of minimum standards for cybersecurity best practices. We support bringing a more coordinated, standardized, and focused approach to how the HPH Sector approaches cybersecurity. The HHS Cyber Performance Goals (CPGs) were an appreciated, proactive step which underscored the collective responsibility to better ensure the resilience of our sector. These are predicated on the best practices co-developed between industry and the federal government pursuant to Section 405(d) of the Cybersecurity Act of 2015.[10] We believe this is a reasonable approach that can help providers improve their cybersecurity posture and resilience.

We respectfully request that this Subcommittee be cognizant that implementing such measures will take time and resources, especially impacting small, medium, and under-resourced providers, and those who were not eligible for electronic health record (EHR) funds, including post-acute and long-term care providers. **CHIME will continue to strongly advocate for the**

[8] 405(d) :: Cornerstone Publications (hhs.gov)
[9] chimecentral.org/content/chime-supports-hhs-release-of-cybersecurity-performance-goals-to-safeguard
[10] hhs_fact_sheet_-_csa_405d_cleared.pdf (nist.gov)

need for financial support to ensure that no one is left behind. An investment in cybersecurity for the healthcare sector will be an investment not just in patient safety but also national security.

Safe Harbors for Threat Information Sharing

Our members have repeatedly reflected how helpful having certain safe harbors would be. Specifically, they have requested that there be protections pertaining to information sharing. There is tremendous fear around information sharing related to when an entity experiences a cyber incident. Far too often the walls go up and organizations are forced to go into a protectionist mode given the significant liability repercussions associated with a data breach. If safe harbors were enacted to shelter organizations experiencing a cyber incident and encourage sharing details of the attack, our entire sector would benefit from the "time is brain" approach. It would move the attack victim from a position of isolation to one where they can freely share threat information for the common good; that will help us all ensure the threat is best contained, managed, and mitigated in timely fashion.

While the Cybersecurity Act of 2015 affords some information sharing, it does not sufficiently remove all the barriers. Stemming from this law, the Department of Homeland Security (DHS) issued guidance that permits threat sharing. However, it limits sharing to the Cybersecurity and Infrastructure Security Agency (CISA), other federal entities, and Information Sharing and Analysis Centers (ISACs) or Information Sharing and Analysis Organizations (ISAOs) and does not entirely inoculate entities from sharing timely critical information about specific threats more widely. For example, we are aware of instances when a hospital experienced a cyberattack and the neighboring hospitals were not made aware because of the liability ramifications. Far too often organizations are counseled early on by their attorneys that they are not permitted to share details of their incident as doing so would open them to significant legal and regulatory risk.

Our members are very concerned they are being unduly penalized instead of being treated as the victim of a crime. Collectively, providers fend off complex attempts at cyber intrusion every day, but it only takes one sophisticated criminal to gain entry. With the increased use of generative AI, criminals are becoming more brazen in weaponizing this new technology. For instance, criminals are taking voice snippets and leveraging generative AI to launch "vishing" (voice phishing) attacks. There has been a 1,265 percent rise in vishing, phishing (email scam) and smishing (scam text) since Chat GPT was introduced.[11]

Finally, we continue to believe that Stark and Anti-Kickback Statutes should be amended to allow for sizeable cyber donations while inoculating donors from risk. Organizations are simply too worried about taking on risk should they donate technology or services, and the recipient later experiences a cyber incident.

All Hazards Designation

As recommended by the Health Sector Coordinating Council (HSCC), high impact cyber and ransomware attacks, which result in the disruption and delay of health care delivery at one or more critical access, safety-net and rural emergency hospitals, should be designated as “all hazards” incidents to activate the Federal Emergency Management Agency (FEMA) and other government response support services.[12] We believe by doing this, more federal resources and support will be available to support our sector when a significant cyber incident occurs.

A major cybersecurity incident should trigger the same level of response as a natural disaster or pandemic given its potential to cripple hospitals and health systems, delay care, and jeopardize patient safety. Further, it can cripple surrounding hospitals and health systems as they must divert the most critical patients elsewhere. The Government Accountability Office (GAO) found that when rural hospitals closed, people living within the community of care coverage areas had to travel about 20 miles farther for common services – including inpatient care.[13]

Mandate Third-Parties and Payers to Share Responsibility

Third-party risk remains an enormous weak spot for the healthcare sector and cannot be solved by imposing costly mandates on providers. Cybersecurity must be a shared responsibility – risk cannot be born alone by providers. Third-parties that store, process and/or transmit protected health information on behalf of HIPAA covered entities are critical to the healthcare sector; yet during each contract negotiation they create caps on their liability that shift multiple millions of dollars of liability for a cybersecurity breach back to those organizations and/or their providers. The number of technological factors and undiscovered vulnerabilities outside of a provider's control is significant. The size of a hospital or healthcare system and their ability to negotiate

[11] https://www.helpnetsecurity.com/2024/02/29/mobile-fraud-losses/

[12] HEALTH-INDUSTRY-CYBERSECURITY-RECOMMENDATIONS-FOR-GOVERNMENT-POLICY-AND-PROGRAMS.pdf (healthsectorcouncil.org)

[13] https://www.gao.gov/products/gao-21-93#summary

these responsibilities with third-parties should not matter. If we are to make meaningful improvements in our sector, this responsibility must be equally shared.

Whether located in a patient's room or the hospital laboratory, both medical devices and other devices – such as a patient's mobile device – rely on network connectivity for operations and maintenance. Additionally, nearly all of the technology components in these devices are not developed by the HDO. These components include software, services, and hardware developed from organizations known as third-parties. One study found that the average number of third-parties that organizations contracted with in 2021 was 1,950 and also anticipated an increase to an average of 2,541 in 2022. Further, it notes that: "Third-party products and services are a necessary and critical part of the HDO IT blueprint, but each brings another set of risk factors to the table. Some risks are inherent to the third-party such as security of operating systems and other embedded software in medical devices […] the risk created by the third-party or the HDO use of the third-party needs to be managed. The burden is on the HDO to perform assessments throughout their relationship with the third-party (e.g., procurement, implementation, usage, updates, termination, etc.)."[14]

Payers and clearinghouses are also HIPAA covered entities. They both hold vast quantities of patient data and are integral partners in the healthcare system as evidenced by the Change Healthcare attack. It is imperative that they meet certain standards as well. Last, we recommend that anyone who is touching health data has an obligation to help protect it. For years, our members have reported to us that they experience challenges with some medical device manufacturers refusing to sign HIPAA BAAs. More details on this can be found in our recent comments to Senator Bill Cassidy in response to his RFI on health data privacy.[15]

Roadmap for the Future

Our sector needs a federally driven "playbook" for the next significant healthcare cyberattack so that we have immediate access to needed information, and federal authorities can help organize outreach and messaging with a strong, clear communication plan. This should include needed clarity for hospitals, healthcare systems, and HDOs on who to call and contact at the start of, during, and after a cyber incident. Put simply, we must have a clear pathway to the federal front-door at HHS. Additionally, we respectfully urge Congress to request that HHS, as the SMRA,

[14] https://assets-global.website-files.com/63bc855e7cb1897eeb806ea7/6532d7b6718a3de763b9cbd1_Ponemon%20Research%20Report%20-%20The%20Impact%20of%20Ransomware%20on%20Healthcare%20During%20COVID-19%20and%20Beyond.pdf

[15] CHIME_Comments_in_Response_to_Sen._Cassidy__R-LA__Request_for_Information_on_Health_Data_Privacy__Oct._2023_.pdf (ctfassets.net)

conduct a sector-wide risk assessment so that we have a clear picture of the inventory of systems, organizations, and interlocking pieces that could be subjected to a cyber incident.

Cyber Insurance Program

The federal government should institute a catastrophic cyber insurance program to help healthcare providers offset the extremely high costs of coverage and serve as a backstop for those unable to obtain insurance on the open market.

The U.S. Department of Treasury has acknowledged that cyber insurance is a significant risk-transfer mechanism, and the insurance industry has an important role to play in strengthening cyber hygiene and building resiliency. In late 2022, Treasury released a Request for Comment regarding a "Potential Federal Insurance Response to Catastrophic Cyber Incidents." CHIME responded to this request, as we strongly believe a federal insurance response to catastrophic cyber incidents in the critical infrastructure sectors is warranted and needed.

Cyber insurance provides coverage for common cyber risks to help companies mitigate losses related to cyber incidents and can encourage policyholders to manage cyber risk. But cyber insurers have been limiting their exposure to systemic losses (including by limiting coverage), and cyber carriers may not fully cover losses from a systemic event with catastrophic losses.

According to our members, based on the annual renewal process they go through – their premiums are continuing to increase, and the average annual increases in premiums that they are experiencing each year have typically doubled, if not more. One member noted that they were paying a $1 million dollar premium for each $5 million dollars of coverage. Some members have reported being denied any cyber insurance coverage – simply because they had experienced a cyberattack within the last five years and are therefore required to "self-insure." Furthermore, even when our members have "comprehensive" cyber insurance, the coverage may only cover half of their losses – often amounting to tens of millions of dollars that they are then left to recoup. A CHIME survey found that nearly 60 percent of our members reported that the Internet of Things (IoT) and connected devices were their largest area of concern for risk of cyber intrusion over the next three years, areas, as described earlier, that can often be outside the HDO's control.

Due to increasing cybersecurity risks, businesses are facing a more demanding underwriting process – and insurers are more thoroughly examining a company's security controls, internal processes, and procedures concerning cyber risk. Additionally, "underwriters are more cautious in examining an insured's risk presented by the third-parties working or contracting with the insured."[16] Hospitals and health systems do not have a choice to simply "not work with" or "not contract with" third-party vendors – yet they are being penalized or deemed uninsurable despite the fact that there is not a streamlined disclosure process to ensure that they are aware of any new potential and/or known vulnerabilities associated with third-party products and/or services. The burden is solely on our members – hospitals and health systems – to perform assessments throughout their relationship with the third-party (e.g., procurement, implementation, usage, updates, termination, and disposition of assets holding patient data).

There are also a myriad of requirements that HDOs must meet to obtain insurance coverage and the requirements vary by carrier. Some requirements do little to improve a provider's cyber posture, yet providers are required to meet them. Therefore, our members believe, based on experience, that the current marketplace for cyber insurance offered to the healthcare sector is tenuous, financially unfeasible, and for some – completely unavailable.

Student Loan Forgiveness Program

Workforce issues continue to plague the healthcare sector and they are also pronounced with a shortage of security professionals. CHIME supports the recommendations made by the HSCC contained in their recent report, "Recommendations for Government Policy and Programs." The report calls for HHS, in conjunction with other federal partners, to administer a workforce development and cyber training program that offers free cyber training and student loan forgiveness programs. They also call for instituting a federally subsidized "civilian cyber health corp" that could offer loan forgiveness in exchange for a minimum number of years served, modeled after a uniformed health corp.

Conclusion:

In closing, thank you again for holding this hearing and for your leadership and attention to the critical issue of healthcare cybersecurity. CHIME remains committed to being a trusted stakeholder and resource as the Subcommittee seeks to improve the cybersecurity posture of the HPH sector.

[16] https://content.naic.org/sites/default/files/cmte-c-cyber-supplement-report-2022-for-data-year-2021.pdf