APPENDIX

MEMORANDUM

TO: Members of the Senate Law and Public Safety Committee

FROM: Christine A. Stearns, chief government relations officer
Neil Eicher, vice president of policy

DATE: December 16, 2024

RE: **The Impact of Cyberattacks on Hospitals**

Thank you for the opportunity to provide testimony on the critical issue of cybersecurity in the healthcare sector and the steps hospitals are taking to respond to recent cyberattacks.

Cyberattacks have become a pressing national security threat, with healthcare among the most targeted sectors. Recent data indicates a 128% surge in cyberattacks in 2023 compared to 2022, with half of these incidents directly compromising patient safety. This trend underscores the urgency of addressing vulnerabilities across the healthcare ecosystem, including not only hospitals but also the third-party entities they rely on.

One stark example is the recent cyberattack on Change Healthcare, a third-party claims processor within the UnitedHealth Group. This attack disrupted critical hospital functions such as claims processing, pharmacy operations, and real-time eligibility verification. The financial repercussions were severe, with claims submissions dropping by $6.3 billion for affected providers in just the first three weeks.

Hospitals struggled to maintain operations, pay staff, procure essential supplies, and ensure patient care amid reduced cash flow and increased administrative burdens. For some, claims disruptions lasted over 60 days, straining resources and operational capacity.

While hospitals are required under the Health Insurance Portability and Accountability Act (HIPAA) to implement comprehensive cybersecurity measures, these attacks highlight the interconnectedness of the healthcare ecosystem. Over 95% of the largest healthcare data breaches in 2023 involved third-party entities, not hospitals themselves.

Hospitals have made significant investments in cybersecurity to safeguard patient data and maintain operational integrity. These efforts include:

- Compliance with Federal Standards: Hospitals adhere to HIPAA and the National Institute of Standards and Technology (NIST) Cybersecurity Framework, ensuring robust administrative, physical, and technical safeguards.
- Risk Assessments: Regular evaluations of potential vulnerabilities, including simulations of cyberattacks.

1x

NJHA Issue Brief: Cybersecurity

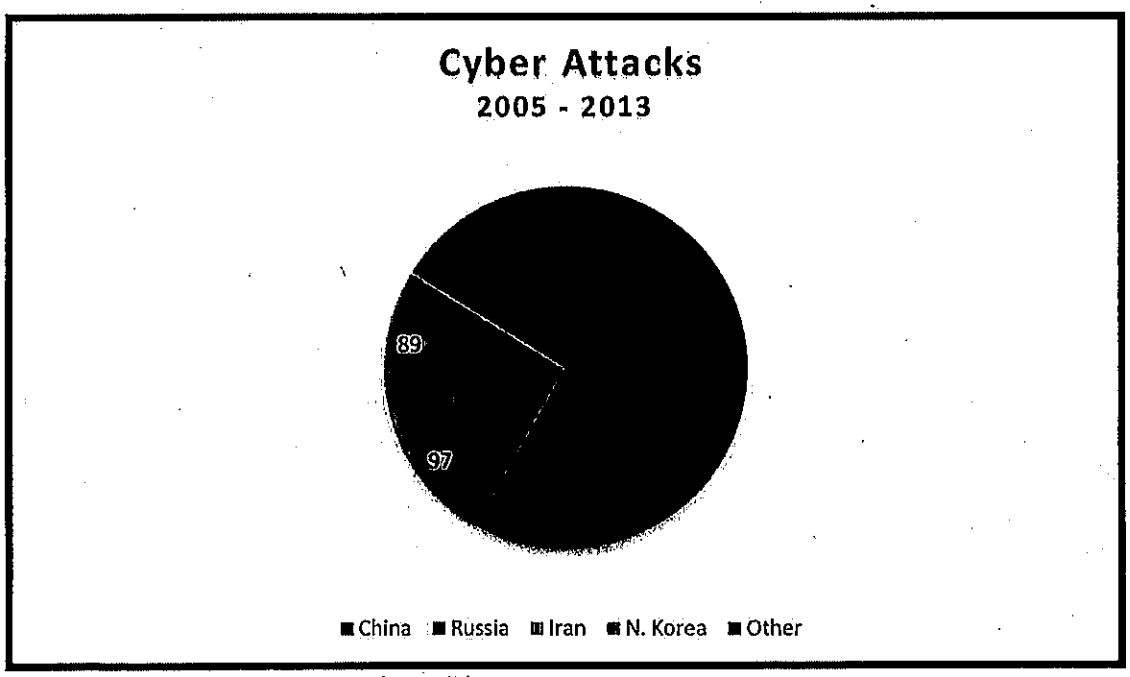
Executive Summary

Cyberattacks are a national threat, and the frequency and depth of these attacks have increased significantly over the last few years. Foreign actors are targeting key sectors of the American economy, such as healthcare, to hold personal information for ransom. These vulnerabilities were highlighted during the recent cyberattack on Change Healthcare, a third-party claims entity, which is part of the UnitedHealth Group. Hospitals depend on third party applications to support key hospital functions, such as claims processing.

Policymakers must act to ensure that these third-party entities meet stringent cybersecurity requirements. In addition, policymakers must ensure that hospitals and health systems have the financial resources to continue to provide necessary care in the event of a cyberattack.

Background

Cyberattacks are a national security threat. Many of the cyberattacks are being conducted by countries that are currently add odds with the United States on foreign affairs. According to the Council on Foreign Relations, 77% of all suspected operations were sponsored by China, Russia, North Korea and Iran.



Source: Council on Foreign Relations, Cyber Incidents 2005-2023

2x

disruptions compelled hospitals, health systems, and other providers to implement workarounds. Additionally, hospitals had to engage new vendors to handle certain claims submission functions. This situation significantly strained their operational capacity and resources.

As a result of the inability to process claims, hospitals, health systems and other providers experienced extraordinary reductions in cash flow. In the March 2024, 94% of hospitals reported that the Change Healthcare cyberattack was impacting them financially, with more than half reporting the impact as "significant or serious."[ii] According to Kodiak Solutions, a revenue cycle data analytics firm, the value of claims submitted dropped $6.3 billion for their 1,850 hospital and 250,000 physician clients in just the first three weeks after the attack.[iii]

The staggering loss of revenue has meant that some hospitals and health systems had to seek alternate ways to ensure they could pay salaries for clinicians and other members of the care team, acquire necessary medicines and supplies, and pay for mission-critical contract work in areas such as physical security, dietary, and environmental services. In addition, replacing previously electronic processes with manual processes has often proved ineffective. This shift added considerable administrative costs for providers, as well as diverting team members from other tasks. Consequently, the burden on healthcare organizations has increased, complicating their operational and financial stability.

Some hospitals experienced claims disruptions for over 60 days before returning to normal operations. The New Jersey Department of Banking and Insurance (DOBI) and the Centers for Medicare and Medicaid Services (CMS) issued directives that required insurance companies to forego normal prior authorization and approval requirements. On March 9, CMS made advanced payments available. However, this reactionary approach to the attack caused unnecessary delays and financial hardships that could have been avoided had there been requirements for these actions already in place.

Hospital Cybersecurity Requirements

Hospitals are legally obligated to protect patient health information (PHI) from cyberattacks, primarily governed by regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States. HIPAA mandates comprehensive safeguards to ensure the confidentiality, integrity, and availability of PHI, including administrative measures like risk assessments and workforce training, physical protections such as secure facility access controls, and technical solutions like encryption and regular security updates. As "covered entities" under HIPAA, hospitals must comply with the HIPAA Security Rule, which encompasses information access management, security incident procedures, and data backup plans, with severe monetary penalties for non-compliance.

Beyond regulatory compliance, hospitals must adopt industry best practices to defend against evolving cyber threats, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Additionally, accrediting bodies like the Joint Commission align their standards with these requirements, and Medicare's Conditions of Participation (CoPs)

3x

introduced legislation that would make entities eligible for Medicare accelerated and advance payment programs due to a cybersecurity incident. This legislation would assist a hospital in being able to receive necessary payments for the functions of their operations in the event that the hospital is significantly affected by a cyberattack.

Congress is also examining requirements for cyber insurance policies. The Insure Cybersecurity Act of 2023 (S.513) establishes a working group to study cyber insurance policies for businesses. The bill highlights the importance of cyber risk management, which impact third-party vendors relied upon by insured companies.

NJHA's Viewpoint

The recent Change Healthcare cyberattack demonstrates the importance of enhancing cybersecurity policies in healthcare. NJHA supports the AHA's position that cybersecurity regulations should focus on the oversight of third-party entities and other entities that handle patient information. Hospitals already invest a significant amount of resources on cybersecurity efforts. NJHA supports voluntary minimum cybersecurity standards for hospitals.

There are several policy reforms that the federal and state governments could consider for protecting against future attacks. They include:

- Enhance the federal government's oversight of healthcare cybersecurity by moving all or part of the oversight to the Department of Homeland Security.
- Hold third-party entities and business associates to a higher standard of "secure by design and secure by default" for technology services and capabilities used in critical healthcare infrastructure. More than half of all data breaches on health systems are through business associates; many ransomware attacks similarly find their way into enterprise networks through third parties.
- Require health insurance companies to develop policies for advanced payments and modified authorization requirements in the event of a cyber incident.
- Reform policies governing liability coverage for medical record companies to better protect them from ransom cyberattacks. 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.
- Require software companies to reduce the cost of cybersecurity protections for non-profit healthcare providers.
- Require the Federal Trade Commission (FTC) to consider cyber readiness during a review of potential health insurer mergers or acquisitions. This includes the acquisition of third-party entities that have access to patient medical records.

Updated: August 14, 2024

4x

CHAMBER OF COMMERCE
SOUTHERN NEW JERSEY
Connecting the region since 1873

[redacted]

MEMORANDUM

TO: **Senate Law and Public Safety Committee**

FROM: Hilary Chebra, Manager, Government Affairs, *CCSNJ*

RE: **Cybersecurity Measures Affecting New Jersey**

DATE: December 16, 2024

The Chamber of Commerce Southern New Jersey (CCSNJ) is the region's largest and most influential business organization representing businesses in the seven most southern counties of New Jersey, as well as greater Philadelphia and northern Delaware. The CCSNJ has approximately 1,200 member companies, of which 85 percent are small businesses that employ less than 50 people, as well as 160 nonprofit members. Thank you for the opportunity to address the critical issue of the growing threat of cybersecurity attacks.

Over recent years, South Jersey businesses of all industries — whether small retailers, manufacturers, healthcare providers, or professional services firms — have faced a sharp uptick in ransomware, phishing, and data breach attempts. Cyberattacks disrupt not only business continuity but also damage consumer confidence and regional economic stability.

Small businesses are often disproportionately affected by these cybersecurity attacks. According to a recent study from Accenture, 43 percent of cyberattacks are aimed at small businesses, and only 14 percent are adequately prepared to defend themselves. Additionally, many lack the resources to recover quickly from these incidents.

With cybersecurity threats becoming increasingly sophisticated and frequent, businesses across the region are taking steps to protect their operations, customers, and data integrity. Many businesses are investing in next-generation firewalls, endpoint protection, and network monitoring tools to identify and mitigate threats in real-time. Regular software updates have become standard practices to address known vulnerabilities swiftly.

Additionally, recognizing that human error is a significant entry point for cybercriminals, companies are implementing cybersecurity awareness trainings. These programs teach employees to recognize phishing attempts, manage passwords securely, and understand the importance of data protection.

Small and mid-sized businesses often lack the resources for in-house IT expertise. Many are increasingly partnering with managed security service providers to oversee threat detection, response, and recovery processes. Collaboration with cybersecurity firms allows businesses to benefit from specialized expertise.

We appreciate the legislature's attention to the business community's challenges in this space. Collaboration with state government is vital to ensuring businesses have the tools necessary to

5x

[redacted]

address this ever-evolving issue. We would like to respectfully recommend the legislature consider legislation creating state-funded cybersecurity grants or tax incentives to help small businesses afford necessary cybersecurity upgrades. As previously mentioned, small businesses are often targeted and have few resources to protect themselves from cyberattacks.

Additionally, we would like to encourage legislation promoting public-private partnerships for cybersecurity training and workforce development. Having a trained workforce in this field is critical to ensuring the resilience and security of our digital infrastructure. By fostering collaboration between government entities, educational institutions, and private sector organizations, we can create comprehensive training programs that address current and emerging cybersecurity threats. This will also help close the growing cybersecurity talent gap. Investing in these partnerships promotes innovation, enhances security, and ensures that businesses and government agencies have access to qualified professionals who can effectively mitigate cyber risks.

We look forward to continued support and stand ready to work with the legislature to provide resources for the business community to maintain robust defenses against the evolving cyber threat landscape.

6x

NJBIA
New Jersey Business & Industry Association

10 W Lafayette Street
Trenton, NJ 08608-2002

609-393-7707
www.njbia.org

Michele N. Siekerka, Esq.
President and CEO

Christopher Emigholz
Chief Government Affairs Officer

Raymond Cantor
Deputy Chief Government Affairs Officer

Althea Ford
Vice President

Elissa Frank
Vice President

Kyle Sullender
Director of Economic Policy Research

To: Chairwoman Greenstein, Vice-Chairman Moriarty, and Members of the Senate Law and Public Safety Committee

From: Kyle Sullender, NJBIA Director of Economic Policy Research (ksullender@njbia.org)

Date: December 16, 2024

RE: NJBIA Testimony regarding business community's response to increasing cybersecurity threats

---

On behalf of our member companies that make NJBIA the largest, most impactful association representing business in New Jersey, we are thankful for the opportunity to submit the following testimony regarding emergent cybersecurity issues and the steps that businesses are actively taking to address a present and ever-increasing threat.

NJBIA's members include some of the nation's largest technology and communications providers in the nation, as well as many small and mid-size businesses that rely on that technology. For all of these companies, despite their diversity in size, scope, and practice, cybersecurity is a serious challenge and one where the need for additional information and resources remains significant.

There are three core factors to this issue that I would like to address:

- Cybersecurity threats are a growing and costly challenge for businesses of all sizes, in all industries.
- Many businesses are adopting proactive prevention strategies to mitigate the risk of significant harm to themselves and their consumers.
- Avoiding future harm caused by malicious actors will require continuing education for members of New Jersey's workforce, as well as investments in public information campaigns and workforce training for information technology professionals.

Threats and Cost - Since the emergence of the COVID-19 pandemic, estimates suggest that cybersecurity attacks have more than doubled. While phishing attempts remain the most common means of attack, the risks posed by more sophisticated methods utilizing new technology, such as artificial intelligence, are increasing.

7A

The monetary risk posed by these threats can be crippling, especially to small businesses. The National Cybersecurity Alliance recently estimated that cyberattacks cost each American entrepreneur approximately $8,000 annually – with the actual costs to impacted businesses being potentially much higher. A report from IBM and the Ponemon Institute estimated that the average cost for a data breach impacting a business with fewer than 500 employees is nearly $3 million.

In light of these challenges, the business community is staying vigilant and innovative to protect consumers' private information and data.

Best Practices and Technological Innovation - As previously noted, the most common form of cyberattacks are broad and targeted phishing attempts. Phishing is an attempt to steal sensitive information like usernames, passwords, or bank information, by fooling a user into willingly entering this information into a fake website or program. This means that the most important prevention strategies are often not technological, but human- and culture-driven.

Solutions offered by employers are varied but often take a similar shape. Some examples include:

- Mandating annual data protection training for all personnel;
- Offering or requiring employee training on threat detection and reporting;
- Conducting periodic phishing simulations to ensure proper response from staff;
- Enforcing stringent guidelines relating to the handling and disposing of sensitive information;
- Performing regular risk assessments with concurrent mitigation strategies;
- Treating cybersecurity as a strategic and customer safety priority, not just an IT concern;
- Integrating cybersecurity into enterprise risk management and governance frameworks; and,
- Employing full-time information security professionals with sufficient authority and independence to proactively and reactively respond to suspected threats.

To further enhance these efforts, technology teams benefit most from an integrated combination of robust security solutions that provide comprehensive protection. This setup could include managed security services from a reliable provider to bolster or supplement the capabilities of internal teams.

In addition to human solutions, firms are developing new software that can detect and prevent cyberattacks. For example, earlier this year AT&T announced the release of its "Dynamic Defense" software which embeds security directly into the networks that its clients rely on to store data and communicate with coworkers, friends, and family. IBM also recently developed new AI-based threat detection software that can better detect when a cyberattack is attempted. And while artificial intelligence is being harnessed by bad actors

to commit attacks, AI technology is also being leveraged to detect and prevent sophisticated strikes.

Workforce Development – What's clear from these and other initiatives is that preventing and responding to cyberattacks requires all workers, not just those in IT, to be well-informed of potential threats and how to avoid them, as well as a well-trained, qualified information security workforce.

With regards to everyday workers, there is a need for continual education, and opportunities exist for public-private partnerships which would increase awareness among New Jersey residents of the evolving ways which cyber criminals are working to gain access to their information and networks and how to prevent it. The National Cybersecurity Alliance is one example of a successful partnership of this kind operating at the national level, which runs a "National Cybersecurity Awareness Month" and "Data Privacy Week" to try to get this critical message to the public. Still, there is a need for continued outreach and information.

With regard to the direct cybersecurity workforce, the Bureau of Labor Statistics projects information security analysts to be the fifth fastest growing occupation in the nation over the next decade. Despite this, a study from the World Economic Forum in 2023 found that few business leaders feel they have the talent they need to meet the evolving threat of cyberattacks.

New Jersey must continue to invest in workforce training programs and opportunities to get qualified cybersecurity professionals into the workforce, as well as to upskill and reskill existing workers who are interested in transitioning into a new career in the field. NJBIA has been a leader in promoting workforce development issues across industries to meet the needs of a changing economy. The NJ Pathways to Career Opportunities Initiative which is led in partnership with the New Jersey Council of Community Colleges is just one such example, and one where training cybersecurity professionals is embedded into one of four strategic areas of focus.

We once again thank the committee and the Chairwoman for holding this hearing and inviting us to participate. Please feel free to email me at ksullender@njbia.org if you have any questions about these comments or future legislation.